vul_files_33 Scan Report

Project Name	vul_files_33
Scan Start	Tuesday, January 7, 2025 5:26:30 PM
Preset	Checkmarx Default
Scan Time	03h:58m:32s
Lines Of Code Scanned	299757
Files Scanned	138
Report Creation Time	Tuesday, January 7, 2025 8:25:40 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035
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

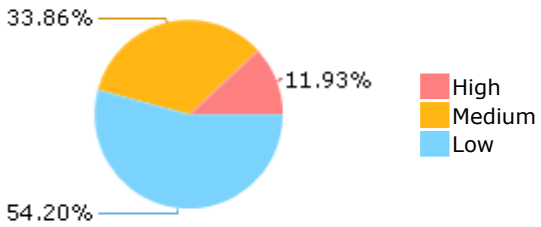
Results Limit

Results limit per query was set to 50

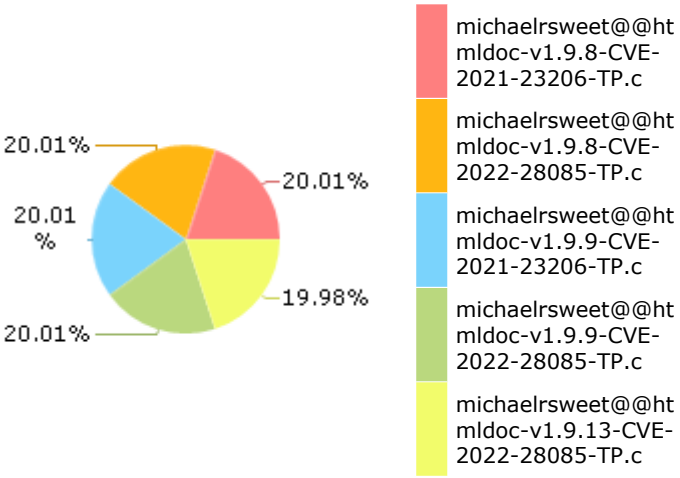
Selected Queries

Selected queries are listed in Result Summary

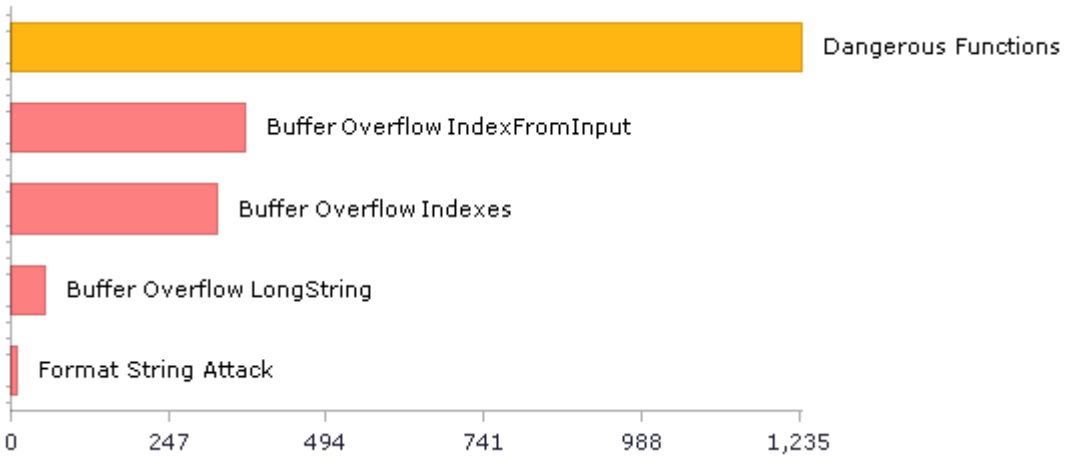
Result Summary



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	1459	463
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	2322	2322
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	43	28
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	3	1
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	1239	1239
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	3	1
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	1	1
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	1239	1239
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	14	14
PCI DSS (3.2) - 6.5.2 - Buffer overflows	1040	420
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.	68	68
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.	58	43
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.	2263	2263
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.	13	13
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.	114	114

***** 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)	2355	2355
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)*	4	4
SC-28 Protection of Information at Rest (P1)	12	12
SC-4 Information in Shared Resources (P1)	1	1
SC-5 Denial of Service Protection (P1)*	418	264
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	970	350
SI-11 Error Handling (P2)*	191	191
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	32	23

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

Scan Summary - 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

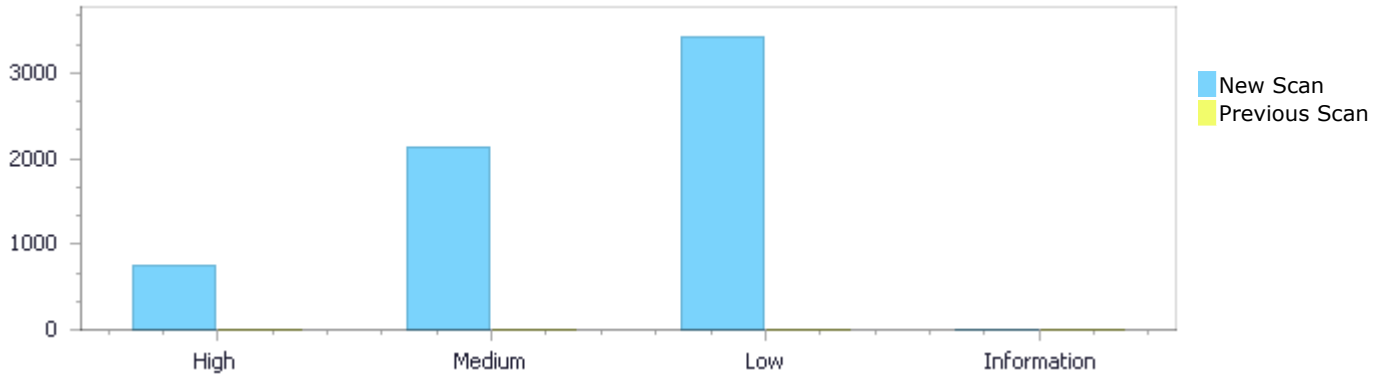
Scan Summary - Custom

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	755	2,142	3,429	0	6,326
Recurrent Issues	0	0	0	0	0
Total	755	2,142	3,429	0	6,326
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	755	2,142	3,429	0	6,326
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	755	2,142	3,429	0	6,326

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	367	High
Buffer Overflow Indexes	324	High
Buffer Overflow LongString	54	High
Format String Attack	10	High
Dangerous Functions	1239	Medium

Buffer Overflow boundcpy WrongSizeParam	215	Medium
Use of Zero Initialized Pointer	136	Medium
Memory Leak	126	Medium
Wrong Size t Allocation	117	Medium
Integer Overflow	114	Medium
MemoryFree on StackVariable	80	Medium
Divide By Zero	63	Medium
Inadequate Encryption Strength	25	Medium
Double Free	18	Medium
Use of Hard coded Cryptographic Key	5	Medium
Use of Uninitialized Pointer	2	Medium
Char Overflow	1	Medium
Heap Inspection	1	Medium
Improper Resource Access Authorization	2254	Low
Heuristic Buffer Overflow malloc	226	Low
Unchecked Return Value	191	Low
NULL Pointer Dereference	153	Low
Unchecked Array Index	145	Low
Sizeof Pointer Argument	93	Low
Heuristic 2nd Order Buffer Overflow malloc	90	Low
TOCTOU	83	Low
Incorrect Permission Assignment For Critical Resources	68	Low
Use of Sizeof On a Pointer Type	52	Low
Exposure of System Data to Unauthorized Control Sphere	33	Low
Potential Off by One Error in Loops	14	Low
Use of Insufficiently Random Values	12	Low
Heuristic 2nd Order Buffer Overflow read	6	Low
Reliance on DNS Lookups in a Decision	4	Low
Potential Path Traversal	3	Low
Improper Resource Shutdown or Release	1	Low
Inconsistent Implementations	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	252
michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	252
michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	252
michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	252
michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	252
michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	86
michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	86
michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	86
michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	86
michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.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=1020042&projectid=20035&pathid=325
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	1133
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1133.             *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=1020042&projectid=20035&pathid=326
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	1133
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1133.              *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=1020042&projectid=20035&pathid=327
Status New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	1133
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1133.            *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=1020042&projectid=20035&pathid=328
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	1133
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1133.            *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=1020042&projectid=20035&pathid=329

Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1133
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.                 color = getc(fp);
....
1133.               *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=1020042&projectid=20035&pathid=330
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1133
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.               temp = getc(fp) & 255;
....
1133.               *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=1020042&projectid=20035&pathid=331
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1133
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.                color = getc(fp);
....
1133.              *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=1020042&projectid=20035&pathid=332
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1133
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1133.             *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=1020042&projectid=20035&pathid=333
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	1130
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1130.              *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=1020042&projectid=20035&pathid=334
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	1130
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1130.                *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=1020042&projectid=20035&pathid=335
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	1130
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1130.               *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=1020042&projectid=20035&pathid=336
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	1130
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1130.               *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=1020042&projectid=20035&pathid=337
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1130
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.                color = getc(fp);
....
1130.                *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=1020042&projectid=20035&pathid=338
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1130
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.              temp = getc(fp) & 255;
....
1130.                *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=1020042&projectid=20035&pathid=339
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1130
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1130.               *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=1020042&projectid=20035&pathid=340
Status New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1130
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1130.               *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=1020042&projectid=20035&pathid=341
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	1129
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1129.                *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=1020042&projectid=20035&pathid=342
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	1129
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1129.                *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=1020042&projectid=20035&pathid=343
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	1129
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1129.                *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=1020042&projectid=20035&pathid=344
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	1129
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1129.                *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=1020042&projectid=20035&pathid=345
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1129
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.               color = getc(fp);
....
1129.               *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=1020042&projectid=20035&pathid=346
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1129
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1129.               *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=1020042&projectid=20035&pathid=347
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

Line	1199	1129
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.                color = getc(fp);
....
1129.                *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=1020042&projectid=20035&pathid=348
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1129
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.              temp = getc(fp) & 255;
....
1129.                *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=1020042&projectid=20035&pathid=349
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1118
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.                 color = getc(fp);
....
1118.               *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=1020042&projectid=20035&pathid=350
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1118
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.               temp = getc(fp) & 255;
....
1118.               *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=1020042&projectid=20035&pathid=351
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1115
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.               color = getc(fp);
....
1115.             *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=1020042&projectid=20035&pathid=352
Status New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1115
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1115.             *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=1020042&projectid=20035&pathid=353
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1114
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.                 color = getc(fp);
....
1114.               *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=1020042&projectid=20035&pathid=354
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1114
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1114.             *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=1020042&projectid=20035&pathid=355
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1223
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1223.           *ptr++ = colormap[temp][0];
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=356
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1223
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1223.           *ptr++ = colormap[temp][0];
```

Buffer Overflow IndexFromInput\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=357
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1220
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1220.             *ptr++ = colormap[temp][1];
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=358
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-	michaelrsweet@@htmldoc-v1.9.16-CVE-

	2022-0137-FP.c	2022-0137-FP.c
Line	1207	1220
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1220.             *ptr++ = colormap[temp][1];
```

Buffer Overflow IndexFromInput\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=359
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1219
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1219.             *ptr++ = colormap[temp][2];
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=360
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1219
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1219.             *ptr++ = colormap[temp][2];
```

Buffer Overflow IndexFromInput\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=361
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1841.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=362
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	1093
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=363
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	1093

Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=364
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=365
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1052	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=366
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1064	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=367
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1159	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=368
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1167	1093
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 45:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=369
Status New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1841.     b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 46:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=370
Status New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 47:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=371
Status New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=372
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	1090
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=373

Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1052	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=374
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1064	1090
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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

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=1020042&projectid=20035&pathid=1
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	1133
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1133.            *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=1020042&projectid=20035&pathid=2
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	1130
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1130.                *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=1020042&projectid=20035&pathid=3
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1129.                *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=1020042&projectid=20035&pathid=4
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	1133
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1133.            *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=1020042&projectid=20035&pathid=5
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	1130
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1130.              *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=1020042&projectid=20035&pathid=6
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1129.               *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=1020042&projectid=20035&pathid=7
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	1133
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1133.              *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=1020042&projectid=20035&pathid=8
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	1130
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1130.              *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=1020042&projectid=20035&pathid=9
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1129.                *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=1020042&projectid=20035&pathid=10
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	1133
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1133.            *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=1020042&projectid=20035&pathid=11
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	1130
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1130.               *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=1020042&projectid=20035&pathid=12
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1129.                *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=1020042&projectid=20035&pathid=13
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1118
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.                  color = getc(fp);
....
1118.              *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=1020042&projectid=20035&pathid=14
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1115

Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.               color = getc(fp);
....
1115.             *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=1020042&projectid=20035&pathid=15
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1114
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.               color = getc(fp);
....
1114.             *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=1020042&projectid=20035&pathid=16
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1133
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.                color = getc(fp);
....
1133.              *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=1020042&projectid=20035&pathid=17
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1130
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.                color = getc(fp);
....
1130.                *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=1020042&projectid=20035&pathid=18
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1092	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1092.               color = getc(fp);
....
1129.               *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=1020042&projectid=20035&pathid=19
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1118
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.               temp = getc(fp) & 255;
....
1118.               *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=1020042&projectid=20035&pathid=20
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1115
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1115.             *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=1020042&projectid=20035&pathid=21
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1114
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1114.             *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=1020042&projectid=20035&pathid=22
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1133
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1133.             *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=1020042&projectid=20035&pathid=23
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1130
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1130.               *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=1020042&projectid=20035&pathid=24
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1104	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1104.             temp = getc(fp) & 255;
....
1129.               *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=1020042&projectid=20035&pathid=25
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-	michaelrsweet@@htmldoc-v1.9.16-CVE-

	2022-0137-FP.c	2022-0137-FP.c
Line	1199	1133
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.                color = getc(fp);
....
1133.              *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=1020042&projectid=20035&pathid=26
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1130
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.                color = getc(fp);
....
1130.                *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=1020042&projectid=20035&pathid=27
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1129.               *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=1020042&projectid=20035&pathid=28
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1223
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1223.           *ptr++ = colormap[temp][0];
```

Buffer Overflow Indexes\Path 29:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=29
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1220
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1220.             *ptr++ = colormap[temp][1];
```

Buffer Overflow Indexes\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=30
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1199	1219
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1199.               color = getc(fp);
....
1219.             *ptr++ = colormap[temp][2];
```

Buffer Overflow Indexes\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=31
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1133
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1207.             temp = getc(fp) & 255;
....
1133.             *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=1020042&projectid=20035&pathid=32
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1130
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1207.             temp = getc(fp) & 255;
....
1130.               *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=1020042&projectid=20035&pathid=33
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1129
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1129.               *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=1020042&projectid=20035&pathid=34
Status	New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1223
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1223.           *ptr++ = colormap[temp][0];
```

Buffer Overflow Indexes\Path 35:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=35
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1207	1220
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1220.             *ptr++ = colormap[temp][1];
```

Buffer Overflow Indexes\Path 36:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=36
Status New

The size of the buffer used by image_load_bmp in temp, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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_bmp passes to getc, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-	michaelrsweet@@htmldoc-v1.9.16-CVE-

	2022-0137-FP.c	2022-0137-FP.c
Line	1207	1219
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
1207.             temp = getc(fp) & 255;
....
1219.             *ptr++ = colormap[temp][2];
```

Buffer Overflow Indexes\Path 37:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=37
Status New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	1093
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 38:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=38
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	1090
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=39
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	1089
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.8-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 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=40
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	1093
Object	getc	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.8-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 41:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=41
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	1090
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=42
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	1089
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=43
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	1093
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=44
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	1090
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=45
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	1089
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=46
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	1093
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=47

Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	1090
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=48
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	1089
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=49
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1052	1078
Object	getc	temp

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-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 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=50
Status	New

The size of the buffer used by image_load_bmp in temp, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1052	1075
Object	getc	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 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=1020042&projectid=20035&pathid=692
Status	New

The size of the buffer used by httpGetHostByName in ip_ptrs, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	733
Object	"127.0.0.1"	ip_ptrs

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=693
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=694
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	753

Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=695
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=696
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 6:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=697
Status New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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=1020042&projectid=20

	035&pathid=698
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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=1020042&projectid=20035&pathid=699
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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=1020042&projectid=20035&pathid=700
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=701
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=702
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	762
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=703
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	763

Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=704
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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=1020042&projectid=20035&pathid=705
Status	New

The size of the buffer used by httpGetHostByName in ip_ptrs, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	733
Object	"127.0.0.1"	ip_ptrs

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 15:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=706
Status New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	763
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 16:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=707
Status New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 17:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=708
Status New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=709
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	762
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=710
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=711
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	761
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=712
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c

Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 22:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=713
Status New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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=1020042&projectid=20035&pathid=714
Status New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 24:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=715
Status New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 25:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=716
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	756
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=717
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 678 of michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	697	753
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=718
Status	New

The size of the buffer used by httpGetHostByName in ip_ptrs, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	685
Object	"127.0.0.1"	ip_ptrs

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
658.        name = "127.0.0.1";
....
685.        ip_ptrs[0]          = (char *)name;
```

Buffer Overflow LongString\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=719
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	703
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=720
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	703
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=721
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c

Line	658	706
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 31:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=722
Status New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	706
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 32:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=723
Status New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	706
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 33:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=724
Status New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	706
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 34:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=725
Status New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	709
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
658.       name = "127.0.0.1";
....
709.       ip_addr = htonl(((((((unsigned)ip[0] << 8) | (unsigned)ip[1])
<< 8) |
```

Buffer Overflow LongString\Path 35:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=726
Status New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	709
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
658.       name = "127.0.0.1";
....
709.       ip_addr = htonl(((((((unsigned)ip[0] << 8) | (unsigned)ip[1])
<< 8) |
```

Buffer Overflow LongString\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=727
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	710
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=728
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	711
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
658.      name = "127.0.0.1";
....
711.                              (unsigned)ip[3]));
```

Buffer Overflow LongString\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=729
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	703
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=730
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.8-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 641 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	658	703

Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=731
Status	New

The size of the buffer used by httpGetHostByName in ip_ptrs, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	685
Object	"127.0.0.1"	ip_ptrs

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
658.      name = "127.0.0.1";
....
685.      ip_ptrs[0]          = (char *)name;
```

Buffer Overflow LongString\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=732
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	709
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
658.       name = "127.0.0.1";
....
709.       ip_addr = htonl(((((((unsigned)ip[0] << 8) | (unsigned)ip[1])
<< 8) |
```

Buffer Overflow LongString\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=733
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	711
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

```
....
658.       name = "127.0.0.1";
....
711.                              (unsigned)ip[3]));
```

Buffer Overflow LongString\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=734
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	710
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=735
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	703
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=736
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	703
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=737
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	703
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=738
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	706
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=739
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	706

Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=740
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	706
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

Buffer Overflow LongString\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=741
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 641 of michaelrsweet@@htmldoc-v1.9.9-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 641 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	658	706
Object	"127.0.0.1"	ip

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpGetHostByName(const char *name) /* I - Hostname or IP address */

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

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=1020042&projectid=20035&pathid=746
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c receives the "%*s%*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%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12634	12634
Object	"%*s%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=747
Status	New

Method write_type1 at line 12403 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c at line 12403.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-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)
```

Format String Attack\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=748
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c receives the "%*s%*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%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 12343.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12574	12574
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12574.        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=1020042&projectid=20035&pathid=749
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c at line 12343.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12590	12590
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12590.        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=1020042&projectid=20035&pathid=750
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c receives the "%*s%*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%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 12343.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12574	12574
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12574.          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=1020042&projectid=20035&pathid=751
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c at line 12343.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12590	12590
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method	write_type1(FILE *out, /* I - File to write to */

```
....
12590.          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=1020042&projectid=20035&pathid=752
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c at line 12343.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c

Line	12574	12574
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12574.          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=1020042&projectid=20035&pathid=753
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c at line 12343.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12590	12590
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12590.          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=1020042&projectid=20035&pathid=754
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c receives the "%*s%*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%*s%d%*s%*s%63s", which is provided as an argument to a string formatting function in write_type1 method of michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c at line 12343.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12574	12574
Object	"%*s%*s%*s%*s%d%*s%*s%63s"	"%*s%*s%*s%*s%d%*s%*s%63s"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12574.          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=1020042&projectid=20035&pathid=755
Status	New

Method write_type1 at line 12343 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-28085-TP.c at line 12343.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12590	12590
Object	"%*s%d%*s%*s%d"	"%*s%d%*s%*s%d"

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12590.          if (sscanf(line, "%*s%d%*s%*s%d", &ch, &width) != 2)
```

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=1020042&projectid=20035&pathid=1266
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	674	674
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
674.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1267
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	688	688
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
688.            memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1268
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	706	706
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
706.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1269
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	721	721
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
721.        memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1270
Status	New

The dangerous function, memcpy, was found in use at line 3596 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3722	3722
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3722.           memcpy(rgb, link_color, sizeof(rgb));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1271
Status	New

The dangerous function, memcpy, was found in use at line 3596 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3771	3771
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3771.           memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1272
Status	New

The dangerous function, memcpy, was found in use at line 3596 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3817	3817
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3817.       memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1273
Status	New

The dangerous function, memcpy, was found in use at line 3964 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4031	4031
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4031.         memcpy(pages[*page].header, Header,
sizeof(pages[*page].header));
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1274
Status	New

The dangerous function, memcpy, was found in use at line 3964 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4032	4032
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4032.         memcpy(pages[*page].header1, Header1,
sizeof(pages[*page].header1));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1275
Status	New

The dangerous function, memcpy, was found in use at line 3964 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4033	4033
Object	memcpy	memcpy

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4033.         memcpy(pages[*page].footer, Footer,
sizeof(pages[*page].footer));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1276
Status	New

The dangerous function, memcpy, was found in use at line 4710 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4807	4807
Object	memcpy	memcpy

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4807.           memcpy(rgb, link_color, sizeof(rgb));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1277
Status	New

The dangerous function, memcpy, was found in use at line 4710 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4891	4891

Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4891.           memcpy(rgb, link_color, sizeof(rgb));
```

Dangerous Functions\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1278
Status New

The dangerous function, memcpy, was found in use at line 4710 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5227	5227
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5227.           memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1279
Status New

The dangerous function, memcpy, was found in use at line 4710 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Line	5395	5395
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5395.         memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1280
Status	New

The dangerous function, memcpy, was found in use at line 5452 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5552	5552
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5552.             memcpy(rgb, link_color, sizeof(rgb));
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1281
Status	New

The dangerous function, memcpy, was found in use at line 5452 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-	michaelrsweet@@htmldoc-v1.9.13-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	5601	5601
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5601.                   memcpy(lineptr, "        ", num_cols);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1282
Status	New

The dangerous function, memcpy, was found in use at line 5452 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5618	5618
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5618.               memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1283
Status	New

The dangerous function, memcpy, was found in use at line 5713 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5802	5802
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_table_row(hdtable_t &table,

```
....
5802.          memcpy(bgrgb, background_color, sizeof(bgrgb));
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1284
Status	New

The dangerous function, memcpy, was found in use at line 5713 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6120	6120
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_table_row(hdtable_t &table,

```
....
6120.      memcpy(bgrgb, background_color, sizeof(bgrgb));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1285
Status	New

The dangerous function, memcpy, was found in use at line 5713 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6186	6186
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_table_row(hdtable_t &table,

```
....
6186.         memcpy(bgrgb, background_color, sizeof(bgrgb));
```

Dangerous Functions\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1286
Status New

The dangerous function, memcpy, was found in use at line 6321 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	7164	7164
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
7164.       memcpy(bgrgb, background_color, sizeof(bgrgb));
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1287
Status New

The dangerous function, memcpy, was found in use at line 8718 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8777	8777
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8777.           memcpy((char *)r->data.text.buffer, (char *)data,
datalen);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1288
Status	New

The dangerous function, memcpy, was found in use at line 8718 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8789	8789
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8789.           memcpy(r->data.box, data, sizeof(r->data.box));
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1289
Status	New

The dangerous function, memcpy, was found in use at line 8718 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8798	8798
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8798.          memcpy((char *)r->data.link, (char *)data, datalen);
```

Dangerous Functions\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1290
Status New

The dangerous function, memcpy, was found in use at line 8836 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8889	8889
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8889.       memcpy(temp, temp - 1, sizeof(page_t));
```

Dangerous Functions\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1291
Status New

The dangerous function, memcpy, was found in use at line 8836 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8898	8898
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8898.       memcpy(temp->header, TocHeader, sizeof(temp->header));
```

Dangerous Functions\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1292
Status New

The dangerous function, memcpy, was found in use at line 8836 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8899	8899
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8899.       memcpy(temp->footer, TocFooter, sizeof(temp->footer));
```

Dangerous Functions\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1293

Status	New

The dangerous function, memcpy, was found in use at line 8836 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8903	8903
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8903.       memcpy(temp->header, Header, sizeof(temp->header));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1294
Status	New

The dangerous function, memcpy, was found in use at line 8836 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8904	8904
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8904.       memcpy(temp->header1, Header1, sizeof(temp->header1));
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=1295
Status	New

The dangerous function, memcpy, was found in use at line 8836 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8905	8905
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8905.       memcpy(temp->footer, Footer, sizeof(temp->footer));
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1296
Status	New

The dangerous function, memcpy, was found in use at line 8836 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8914	8914
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8914.       memcpy(temp->background_color, background_color,
```

Dangerous Functions\Path 32:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1297
Status	New

The dangerous function, memcpy, was found in use at line 9557 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9577	9577
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9577.          memcpy(temp, t, sizeof(tree_t));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1298
Status	New

The dangerous function, memcpy, was found in use at line 9557 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9594	9594
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9594.            memcpy(temp, t, sizeof(tree_t));
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1299
Status	New

The dangerous function, memcpy, was found in use at line 10020 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	10088	10088
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method ps_ascii85(FILE *out, /* I - File to print to */

```
....
10088.        memcpy(leftdata + leftcount, data, (size_t)(length -
leftcount));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1300
Status	New

The dangerous function, memcpy, was found in use at line 11300 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11737	11737
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11737.      memcpy(user_pad + i, pad, (size_t)(32 - i));
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1301
Status	New

The dangerous function, memcpy, was found in use at line 11300 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11748	11748
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11748.        memcpy(owner_pad + i, pad, (size_t)(32 - i));
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1302
Status	New

The dangerous function, memcpy, was found in use at line 11300 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11793	11793
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11793.          memcpy(owner_key, user_pad, 32);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1303
Status	New

The dangerous function, memcpy, was found in use at line 11300 in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11855	11855
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11855.        memcpy(encrypt_key, digest, (size_t)encrypt_len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1304
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	674	674
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1305
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	688	688
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1306
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	706	706
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1307
Status	New

The dangerous function, memcpy, was found in use at line 373 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	721	721
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1308
Status	New

The dangerous function, memcpy, was found in use at line 3594 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3718	3718
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1309
Status	New

The dangerous function, memcpy, was found in use at line 3594 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3767	3767
Object	memcpy	memcpy

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1310
Status	New

The dangerous function, memcpy, was found in use at line 3594 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3813	3813
Object	memcpy	memcpy

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	render_contents(tree_t *t, /* I - Tree to parse */

```
....
3813.       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=1020042&projectid=20035&pathid=1311
Status	New

The dangerous function, memcpy, was found in use at line 3951 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4018	4018
Object	memcpy	memcpy

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-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));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1312
Status	New

The dangerous function, memcpy, was found in use at line 3951 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4019	4019
Object	memcpy	memcpy

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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));
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1313
Status	New

The dangerous function, memcpy, was found in use at line 3951 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4020	4020
Object	memcpy	memcpy

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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));
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1314
Status	New

The dangerous function, memcpy, was found in use at line 4686 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c

Line	4783	4783
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4783.           memcpy(rgb, link_color, sizeof(rgb));
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1315
Status New

The dangerous function, memcpy, was found in use at line 4686 in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4867	4867
Object	memcpy	memcpy

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4867.           memcpy(rgb, link_color, 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=1020042&projectid=20035&pathid=756

Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	674	674
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=757
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	688	688
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=758
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	706	706
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=759
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	721	721
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=760
Status	New

The size of the buffer used by render_contents in rgb, at line 3596 of michaelrsweet@@htmldoc-v1.9.13-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 3596 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3771	3771
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=761
Status	New

The size of the buffer used by render_contents in rgb, at line 3596 of michaelrsweet@@htmldoc-v1.9.13-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 3596 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3817	3817
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3817.      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=1020042&projectid=20035&pathid=762
Status	New

The size of the buffer used by parse_doc in pages, at line 3964 of michaelrsweet@@htmldoc-v1.9.13-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 3964 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4031	4031
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4031.         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=1020042&projectid=20035&pathid=763
Status	New

The size of the buffer used by parse_doc in page, at line 3964 of michaelrsweet@@htmldoc-v1.9.13-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 3964 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4031	4031
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4031.         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=1020042&projectid=20035&pathid=764
Status	New

The size of the buffer used by parse_doc in pages, at line 3964 of michaelrsweet@@htmldoc-v1.9.13-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 3964 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4032	4032
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4032.         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=1020042&projectid=20035&pathid=765
Status	New

The size of the buffer used by parse_doc in page, at line 3964 of michaelrsweet@@htmldoc-v1.9.13-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 3964 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4032	4032
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4032.         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=1020042&projectid=20035&pathid=766
Status	New

The size of the buffer used by parse_doc in pages, at line 3964 of michaelrsweet@@htmldoc-v1.9.13-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 3964 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4033	4033
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4033.         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=1020042&projectid=20035&pathid=767
Status	New

The size of the buffer used by parse_doc in page, at line 3964 of michaelrsweet@@htmldoc-v1.9.13-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 3964 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4033	4033
Object	page	page

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	parse_doc(tree_t *t, /* I - Tree to parse */

```
....
4033.         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=1020042&projectid=20035&pathid=768
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4710 of michaelrsweet@@htmldoc-v1.9.13-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 4710 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5227	5227
Object	rgb	rgb

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5227.           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=1020042&projectid=20035&pathid=769
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4710 of michaelrsweet@@htmldoc-v1.9.13-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 4710 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5395	5395

Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5395.         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=1020042&projectid=20035&pathid=770
Status	New

The size of the buffer used by parse_pre in rgb, at line 5452 of michaelrsweet@@htmldoc-v1.9.13-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 5452 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5618	5618
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5618.               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=1020042&projectid=20035&pathid=771
Status	New

The size of the buffer used by new_render in Namespace834634149, at line 8718 of michaelrsweet@@htmldoc-v1.9.13-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 Namespace834634149, at line 8718 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-	michaelrsweet@@htmldoc-v1.9.13-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	8789	8789
Object	Namespace834634149	Namespace834634149

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method new_render(int page, /* I - Page number (0-n) */

```
....
8789.          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=1020042&projectid=20035&pathid=772
Status	New

The size of the buffer used by check_pages in ->, at line 8836 of michaelrsweet@@htmldoc-v1.9.13-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 8836 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8898	8898
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8898.       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=1020042&projectid=20035&pathid=773
Status	New

The size of the buffer used by check_pages in ->, at line 8836 of michaelrsweet@@htmldoc-v1.9.13-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 8836 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8899	8899
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8899.       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=1020042&projectid=20035&pathid=774
Status	New

The size of the buffer used by check_pages in ->, at line 8836 of michaelrsweet@@htmldoc-v1.9.13-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 8836 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8903	8903
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8903.       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=1020042&projectid=20035&pathid=775
Status	New

The size of the buffer used by check_pages in ->, at line 8836 of michaelrsweet@@htmldoc-v1.9.13-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 8836 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8904	8904
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8904.       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=1020042&projectid=20035&pathid=776
Status	New

The size of the buffer used by check_pages in ->, at line 8836 of michaelrsweet@@htmldoc-v1.9.13-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 8836 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8905	8905
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8905.       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=1020042&projectid=20035&pathid=777
Status	New

The size of the buffer used by check_pages in ->, at line 8836 of michaelrsweet@@htmldoc-v1.9.13-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 8836 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8915	8915
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page) // I - Current page

```
....
8915.                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=1020042&projectid=20035&pathid=778
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	674	674
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=779
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	688	688
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=780
Status New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	706	706
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=781
Status New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	721	721
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=782
Status New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3767	3767
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=783

Status	New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3813	3813
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=784
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4018	4018
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 30:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=785
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4018	4018
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=786
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4019	4019
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=787
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4019	4019
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=788
Status	New

The size of the buffer used by parse_doc in pages, at line 3951 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4020	4020
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=789
Status	New

The size of the buffer used by parse_doc in page, at line 3951 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4020	4020
Object	page	page

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=790
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5203	5203
Object	rgb	rgb

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=791
Status	New

The size of the buffer used by parse_paragraph in rgb, at line 4686 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5371	5371
Object	rgb	rgb

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=792
Status	New

The size of the buffer used by parse_pre in rgb, at line 5428 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5590	5590
Object	rgb	rgb

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5590.             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=1020042&projectid=20035&pathid=793
Status	New

The size of the buffer used by new_render in Namespace606042922, at line 8662 of michaelrsweet@@htmldoc-v1.9.8-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 Namespace606042922, at line 8662 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8733	8733
Object	Namespace606042922	Namespace606042922

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	new_render(int page, /* I - Page number (0-n) */

```
....
8733.           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=1020042&projectid=20035&pathid=794
Status	New

The size of the buffer used by check_pages in ->, at line 8780 of michaelrsweet@@htmldoc-v1.9.8-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 8780 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c

Line	8842	8842
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8842.       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=1020042&projectid=20035&pathid=795
Status	New

The size of the buffer used by check_pages in ->, at line 8780 of michaelrsweet@@htmldoc-v1.9.8-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 8780 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8843	8843
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8843.       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=1020042&projectid=20035&pathid=796
Status	New

The size of the buffer used by check_pages in ->, at line 8780 of michaelrsweet@@htmldoc-v1.9.8-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 8780 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-	michaelrsweet@@htmldoc-v1.9.8-CVE-

	2021-23206-TP.c	2021-23206-TP.c
Line	8847	8847
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8847.       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=1020042&projectid=20035&pathid=797
Status	New

The size of the buffer used by check_pages in ->, at line 8780 of michaelrsweet@@htmldoc-v1.9.8-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 8780 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8848	8848
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8848.       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=1020042&projectid=20035&pathid=798
Status	New

The size of the buffer used by check_pages in ->, at line 8780 of michaelrsweet@@htmldoc-v1.9.8-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 8780 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8849	8849
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8849.       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=1020042&projectid=20035&pathid=799
Status	New

The size of the buffer used by check_pages in ->, at line 8780 of michaelrsweet@@htmldoc-v1.9.8-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 8780 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8859	8859
Object	->	->

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8859.               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=1020042&projectid=20035&pathid=800
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	674	674
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=801
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	688	688
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=802
Status	New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	706	706
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=803
Status New

The size of the buffer used by pspdf_export in rgb, at line 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	721	721
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=804
Status New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	3767	3767
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=805
Status New

The size of the buffer used by render_contents in rgb, at line 3594 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	3813	3813
Object	rgb	rgb

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3813.      memcpy(r->data.text.rgb, rgb, sizeof(rgb));
```

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=1020042&projectid=20035&pathid=3353
Status	New

The variable declared in current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	171
Object	current_palette	current_palette

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
171.                          putc(current_palette[i].r, ftga);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3354
Status	New

The variable declared in current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	171
Object	current_palette	current_palette

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
171.                          putc(current_palette[i].r, ftga);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3355
Status	New

The variable declared in current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	170
Object	current_palette	current_palette

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
170.                          putc(current_palette[i].g, ftga);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3356
Status	New

The variable declared in current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	169
Object	current_palette	current_palette

Code Snippet

File Name	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method	int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
169.                          putc(current_palette[i].b, ftga);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3357
Status	New

The variable declared in current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	170
Object	current_palette	current_palette

Code Snippet

File Name	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method	int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
170.                          putc(current_palette[i].g, ftga);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3358
Status	New

The variable declared in current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	169
Object	current_palette	current_palette

Code Snippet	
File Name	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method	int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
169.                            putc(current_palette[i].b, ftga);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3359
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c in line 355 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c in line 355.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	357	398
Object	re_compile	compiled

Code Snippet	
File Name	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method	static int _load_python_objects(PyObject* module) {

```
....
357.      PyObject* re_compile = NULL;
....
398.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3360
Status	New

The variable declared in id at mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c in line 1772 is not initialized when it is used by value at mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c in line 1772.

	Source	Destination

File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	2254	2292
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2254.               PyObject* id = NULL;
....
2292.                   value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3361
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c in line 355 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c in line 355.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	357	398
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
357.      PyObject* re_compile = NULL;
....
398.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3362
Status	New

The variable declared in id at mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c in line 1772 is not initialized when it is used by value at mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c in line 1772.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	2254	2292
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2254.              PyObject* id = NULL;
....
2292.                  value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3363
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c in line 355 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c in line 355.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	357	398
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
357.      PyObject* re_compile = NULL;
....
398.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3364
Status	New

The variable declared in id at mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c in line 1772 is not initialized when it is used by value at mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c in line 1772.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	2254	2292
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2254.               PyObject* id = NULL;
....
2292.                   value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3365
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c in line 355 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c in line 355.

	Source	Destination
File	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Line	357	398
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
357.      PyObject* re_compile = NULL;
....
398.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3366
Status	New

The variable declared in id at mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c in line 1772 is not initialized when it is used by value at mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c in line 1772.

	Source	Destination
File	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Line	2254	2292
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2254.              PyObject* id = NULL;
....
2292.                  value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3367
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 354 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 354.

	Source	Destination
File	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Line	356	396

Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
356.      PyObject* re_compile = NULL;
....
396.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3368
Status	New

The variable declared in id at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 1750 is not initialized when it is used by value at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 1750.

	Source	Destination
File	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Line	2232	2270
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2232.              PyObject* id = NULL;
....
2270.                  value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3369
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 329 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 329.

	Source	Destination
File	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Line	331	364
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
331.      PyObject* re_compile = NULL;
....
364.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3370
Status	New

The variable declared in ret at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 1512 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 1574.

	Source	Destination
File	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Line	1519	1653
Object	ret	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Method static PyObject *_dbref_hook(PyObject* self, PyObject* value) {

```
....
1519.      PyObject* ret = NULL;
```

File Name mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
1653.              value = _dbref_hook(self, value);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3371
Status	New

The variable declared in id at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 1574 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 1574.

	Source	Destination
File	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Line	1994	2032
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
1994.               PyObject* id = NULL;
....
2032.                   value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3372
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 327 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 327.

	Source	Destination
File	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Line	329	361
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
329.      PyObject* re_compile = NULL;
....
361.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3373
Status	New

The variable declared in ret at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 1495 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 1557.

	Source	Destination
File	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Line	1502	1636
Object	ret	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Method static PyObject *_dbref_hook(PyObject* self, PyObject* value) {

```
....
1502.      PyObject* ret = NULL;
```

File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
1636.              value = _dbref_hook(self, value);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3374
Status	New

The variable declared in id at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 1557 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 1557.

	Source	Destination
File	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Line	1977	2015
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
1977.               PyObject* id = NULL;
....
2015.                   value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3375
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 465 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 465.

	Source	Destination
File	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Line	467	505
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
467.      PyObject* re_compile = NULL;
....
505.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3376

Status	New

The variable declared in ret at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 1645 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 1707.

	Source	Destination
File	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Line	1652	1786
Object	ret	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Method static PyObject *_dbref_hook(PyObject* self, PyObject* value) {

```
....
1652.       PyObject* ret = NULL;
```

File Name mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
1786.               value = _dbref_hook(self, value);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3377
Status	New

The variable declared in id at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 1707 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 1707.

	Source	Destination
File	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Line	2207	2245
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2207.              PyObject* id = NULL;
....
2245.                  value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3378
Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 521 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 521.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Line	523	587
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
523.      PyObject* re_compile = NULL;
....
587.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3379
Status	New

The variable declared in ret at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 1758 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 1820.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Line	1765	1899

Object	ret	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Method static PyObject *_dbref_hook(PyObject* self, PyObject* value) {

```
....
1765.       PyObject* ret = NULL;
```

File Name mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c

Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
1899.              value = _dbref_hook(self, value);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3380
Status	New

The variable declared in id at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 1820 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 1820.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Line	2325	2363
Object	id	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Method static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2325.              PyObject* id = NULL;
....
2363.                  value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3381

Status	New

The variable declared in re_compile at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 521 is not initialized when it is used by compiled at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 521.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Line	523	587
Object	re_compile	compiled

Code Snippet
File Name mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Method static int _load_python_objects(PyObject* module) {

```
....
523.      PyObject* re_compile = NULL;
....
587.      compiled = PyObject_CallFunction(re_compile, "O",
empty_string);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3382
Status	New

The variable declared in ret at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 1758 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 1820.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Line	1765	1899
Object	ret	value

Code Snippet
File Name mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Method static PyObject *_dbref_hook(PyObject* self, PyObject* value) {

```
....
1765.      PyObject* ret = NULL;
```

File Name mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c

Method	static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
1899.              value = _dbref_hook(self, value);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3383
Status	New

The variable declared in id at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 1820 is not initialized when it is used by value at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 1820.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Line	2325	2363
Object	id	value

Code Snippet	
File Name	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Method	static PyObject* get_value(PyObject* self, PyObject* name, const char* buffer,

```
....
2325.              PyObject* id = NULL;
....
2363.                  value = PyObject_CallFunctionObjArgs(dbref_type,
collection, id, NULL);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3384
Status	New

The variable declared in tc at mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c in line 17 is not initialized when it is used by e at mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c in line 62.

	Source	Destination
File	mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c	mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c
Line	24	77
Object	tc	e

Code Snippet
File Name mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c
Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
24.      struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c

Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
77.        e->c = tc;
```

Use of Zero Initialized Pointer\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3385
Status New

The variable declared in tc at mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c in line 17 is not initialized when it is used by e at mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c in line 62.

	Source	Destination
File	mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c	mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c
Line	24	81
Object	tc	e

Code Snippet
File Name mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c
Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
24.      struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.1-rc-CVE-2021-4110-FP.c

Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
81.        e->mid = MRB_PROC_ENV(up)->mid;
```

Use of Zero Initialized Pointer\Path 34:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3386
Status	New

The variable declared in tc at mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c in line 17 is not initialized when it is used by e at mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c in line 62.

	Source	Destination
File	mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c	mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c
Line	24	77
Object	tc	e

Code Snippet
File Name mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c
Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
24.      struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c
Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
77.        e->c = tc;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3387
Status	New

The variable declared in tc at mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c in line 17 is not initialized when it is used by e at mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c in line 62.

	Source	Destination
File	mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c	mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c
Line	24	81
Object	tc	e

Code Snippet
File Name mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c
Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
24.      struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.1-rc-CVE-2022-0080-FP.c

Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
81.        e->mid = MRB_PROC_ENV(up)->mid;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3388
Status	New

The variable declared in tc at mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c in line 18 is not initialized when it is used by e at mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c in line 63.

	Source	Destination
File	mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c	mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c
Line	25	78
Object	tc	e

Code Snippet

File Name mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c

Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
25.      struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c

Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
78.        e->c = tc;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3389
Status	New

The variable declared in tc at mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c in line 18 is not initialized when it is used by e at mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c in line 63.

	Source	Destination
File	mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c	mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c
Line	25	82
Object	tc	e

Code Snippet
File Name mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c
Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
25.      struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.2-rc2-CVE-2021-4110-FP.c
Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
82.        e->mid = MRB_PROC_ENV(up)->mid;
```

Use of Zero Initialized Pointer\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3390
Status New

The variable declared in tc at mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c in line 18 is not initialized when it is used by e at mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c in line 63.

	Source	Destination
File	mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c	mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c
Line	25	78
Object	tc	e

Code Snippet
File Name mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c
Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
25.      struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c

Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
78.         e->c = tc;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3391
Status	New

The variable declared in tc at mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c in line 18 is not initialized when it is used by e at mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c in line 63.

	Source	Destination
File	mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c	mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c
Line	25	82
Object	tc	e

Code Snippet

File Name mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c

Method mrb_proc_new(mrb_state *mrb, mrb_irep *irep)

```
....
25.       struct RClass *tc = NULL;
```

File Name mruby@@mruby-2.1.2-rc2-CVE-2022-0080-FP.c

Method closure_setup(mrb_state *mrb, struct RProc *p)

```
....
82.         e->mid = MRB_PROC_ENV(up)->mid;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3392
Status	New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3393
Status New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3394
Status New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3395
Status New

The variable declared in pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	523	726
Object	pages	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 44:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3396
Status	New

The variable declared in height_var at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 6321 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 5713.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	7047	5716
Object	height_var	height_var

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Method parse_table(tree_t *t, // I - Tree to parse

```
....
7047.      height_var = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Method render_table_row(hdtable_t &table,

```
....
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=1020042&projectid=20035&pathid=3397
Status	New

The variable declared in height_var at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 5713 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 5713.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5945	5716
Object	height_var	height_var

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Method	render_table_row(hdtable_t &table,

```
....
5945.      height_var = NULL;
....
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=1020042&projectid=20035&pathid=3398
Status	New

The variable declared in cells at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 6321 is not initialized when it is used by height_var at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 5713.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6396	5716
Object	cells	height_var

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6396.    cells = NULL;
```

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	render_table_row(hdtable_t &table,

```
....
5716.                   uchar     *height_var,
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3399
Status	New

The variable declared in next at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 8718 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 8718.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8820	8822
Object	next	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3400
Status New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c in line 705 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c in line 705.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	755	836
Object	match	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
755.       match = NULL;
....
836.       images[num_images] = img;
```

Use of Zero Initialized Pointer\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3401
Status New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c in line 705 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c in line 705.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	755	822
Object	match	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
755.      match = NULL;
....
822.        images = temp;
```

Use of Zero Initialized Pointer\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3402
Status New

The variable declared in match at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c in line 676 is not initialized when it is used by images at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c in line 676.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	726	807
Object	match	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
726.      match = NULL;
....
807.      images[num_images] = img;
```

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=1020042&projectid=20035&pathid=3225
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3145	3145
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_start_object(FILE *out, // I - File to write to

```
....
3145.         temp = (int *)malloc(sizeof(int) * alloc_objects);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3226
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4640	4640
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4640.           temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=3227
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4659	4659
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_heading(tree_t *t, /* I - Tree to parse */

```
....
4659.           temp = (int *)malloc(sizeof(int) * alloc_headings);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3228
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8852	8852
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method check_pages(int page)   // I - Current page

```
....
8852.         temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3229
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Line	8953	8953
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8953.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Memory Leak\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3230
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9576	9576
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9576.          temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3231
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9593	9593
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Method	flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9593.           temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3232
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9632	9632
Object	temp	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9632.         temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3233
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	1080	1080
Object	temp	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method	file_temp(char *name, /* O - Filename */

```
....
1080.         temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3234
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	1127	1127
Object	name	name

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_temp(char *name, /* O - Filename */

```
....
1127.    temp->name = strdup(name);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3235
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	438	438
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
438.        web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3236
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	585	585
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
585.      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=1020042&projectid=20035&pathid=3237
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	965	965
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    img->pixels = (uchar *)malloc((size_t)(img->width * img->height
* img->depth));
```

Memory Leak\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3238
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1373	1373

Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1373.            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=1020042&projectid=20035&pathid=3239
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1465	1465
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_jpeg(image_t *img, /* I - Image pointer */

```
....
1465.    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=1020042&projectid=20035&pathid=3240
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1786	1786
Object	mask	mask

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

Method	image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1786.    img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3241
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	1080	1080
Object	temp	temp

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method	file_temp(char *name, /* O - Filename */

```
....
1080.        temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3242
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	1127	1127
Object	name	name

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method	file_temp(char *name, /* O - Filename */

```
....
1127.    temp->name = strdup(name);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3243
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	438	438
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
438.        web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3244
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	585	585
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
585.      web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3245
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	1080	1080
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_temp(char *name, /* O - Filename */

```
....
1080.         temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Memory Leak\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3246
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	1127	1127
Object	name	name

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_temp(char *name, /* O - Filename */

```
....
1127.     temp->name = strdup(name);
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3247
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	438	438

Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
438.        web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3248
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	585	585
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
585.      web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3249
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	1075	1075
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1075.        temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3250
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	1122	1122
Object	name	name

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1122.    temp->name = strdup(name);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3251
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	434	434
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
434.        web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 28:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3252
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	595	595
Object	url	url

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
595.      web_cache[web_files - 1].url = strdup(filename);
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3253
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	925	925
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3254
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3255
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1395	1395
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3256
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

Line	1701	1701
Object	mask	mask

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3257
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3143	3143
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3258
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4616	4616
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3259
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4635	4635
Object	temp	temp

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3260
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8796	8796
Object	temp	temp

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	check_pages(int page) // I - Current page

```
....
8796.        temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3261
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8897	8897
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8897.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3262
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	9519	9519
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9519.          temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3263
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	9536	9536
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9536.           temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3264
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	9575	9575
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method flatten_tree(tree_t *t) /* I - Markup tree to flatten */

```
....
9575.           temp = (tree_t *)calloc(sizeof(tree_t), 1);
```

Memory Leak\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3265
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	925	925

Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3266
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3267
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1395	1395
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3268
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1701	1701
Object	mask	mask

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Method	image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3269
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	925	925
Object	pixels	pixels

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3270
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3271
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1395	1395
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 48:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3272
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1701	1701
Object	mask	mask

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    img->mask = (uchar *)calloc(size, 1);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3273
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	925	925
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3274
Status	New

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1326	1326
Object	pixels	pixels

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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));
```

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=1020042&projectid=20035&pathid=1034
Status	New

The function valuelen in michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c at line 553 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@@pdfio-v1.0.0-CVE-2023-24808-TP.c	michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c
Line	570	570
Object	valuelen	valuelen

Code Snippet
File Name michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c
Method pdfioDictSetBinary(

```
....
570.    if ((temp.value.binary.data = (unsigned char *)malloc(valuelen))
== NULL)
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1035
Status	New

The function filesize in miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c at line 11 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	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	88	88
Object	filesize	filesize

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
88.   buffer = malloc(filesize);
```

Wrong Size t Allocation\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1036
Status New

The function size in michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c at line 1757 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-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1786	1786
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1786.    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=1020042&projectid=20035&pathid=1037

Status	New

The function size in michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c at line 1672 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-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20035&pathid=1038
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c at line 1672 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-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20

	035&pathid=1039
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c at line 1672 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-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20035&pathid=1040
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c at line 1672 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-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20035&pathid=1041
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c at line 1672 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-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20035&pathid=1042
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c at line 1672 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-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20035&pathid=1043
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c at line 1672 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-v1.9.9-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20035&pathid=1044
Status	New

The function size in michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c at line 1672 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-v1.9.9-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Line	1701	1701
Object	size	size

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Method image_need_mask(image_t *img, /* I - Image to add mask to */

```
....
1701.    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=1020042&projectid=20035&pathid=1045
Status	New

The function need in mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c at line 822 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	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	947	947
Object	need	need

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method sink(int argc, char **argv)

```
....
947.                            namebuf = xmalloc(need);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1046
Status	New

The function size in mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c at line 1219 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	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	1238	1238
Object	size	size

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method allocbuf(BUF *bp, int fd, int blksize)

```
....
1238.             bp->buf = xmalloc(size);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1047
Status	New

The function size in mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c at line 1219 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	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	1240	1240
Object	size	size

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method allocbuf(BUF *bp, int fd, int blksize)

```
....
1240.             bp->buf = xrealloc(bp->buf, size);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1048
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1258.    outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1049
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3145	3145
Object	alloc_objects	alloc_objects

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1050
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4640	4640
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1051
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4659	4659
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1052
Status	New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8852	8852
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1053
Status	New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	8953	8953
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1054
Status	New

The function web_alloc in michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.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-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	1080	1080
Object	web_alloc	web_alloc

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c

Method	file_temp(char *name, /* O - Filename */

```
....
1080.         temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1055
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c at line 705 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-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	809	809
Object	alloc_images	alloc_images

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load(const char *filename,/* I - Name of image file */

```
....
809.         temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1056
Status	New

The function web_alloc in michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.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-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	1080	1080
Object	web_alloc	web_alloc

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method	file_temp(char *name, /* O - Filename */

```
....
1080.         temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1057
Status	New

The function web_alloc in michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.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-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	1080	1080
Object	web_alloc	web_alloc

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method	file_temp(char *name, /* O - Filename */

```
....
1080.         temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1058
Status	New

The function web_alloc in michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c at line 1055 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-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	1075	1075
Object	web_alloc	web_alloc

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1075.         temp = (cache_t *)malloc(sizeof(cache_t) * web_alloc);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1059
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1060
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	pspdf_prepare_outpages()

```
....
1258.    outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1061
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3143	3143
Object	alloc_objects	alloc_objects

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1062
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4616	4616

Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1063
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4635	4635
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1064
Status	New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 8780 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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c

Line	8796	8796
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method check_pages(int page) // I - Current page

```
....
8796.         temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1065
Status	New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 8871 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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	8897	8897
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8897.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1066
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-	michaelrsweet@@htmldoc-v1.9.8-CVE-

	2022-0137-TP.c	2022-0137-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1067
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1068
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1069
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1258.     outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1070
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	3143	3143
Object	alloc_objects	alloc_objects

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1071
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	4616	4616
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1072
Status	New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	4635	4635
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1073
Status New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 8780 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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	8796	8796
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method check_pages(int page)   // I - Current page

```
....
8796.        temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Wrong Size t Allocation\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1074
Status New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 8871 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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	8897	8897
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8897.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Wrong Size t Allocation\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1075
Status New

The function web_alloc in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	1063	1063
Object	web_alloc	web_alloc

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1076
Status New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1077
Status	New

The function num_pages in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	1258	1258
Object	num_pages	num_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1258.    outpages = (outpage_t *)malloc(sizeof(outpage_t) * num_pages);
```

Wrong Size t Allocation\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1078
Status	New

The function alloc_objects in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	3143	3143
Object	alloc_objects	alloc_objects

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1079
Status New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	4616	4616
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1080
Status New

The function alloc_headings in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	4635	4635
Object	alloc_headings	alloc_headings

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1081
Status New

The function alloc_pages in michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c at line 8780 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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	8796	8796
Object	alloc_pages	alloc_pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method check_pages(int page)   // I - Current page

```
....
8796.        temp = (page_t *)malloc(sizeof(page_t) * alloc_pages);
```

Wrong Size t Allocation\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1082
Status New

The function alloc_links in michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c at line 8871 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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	8897	8897
Object	alloc_links	alloc_links

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method add_link(uchar *name, /* I - Name of link */

```
....
8897.          temp = (link_t *)malloc(sizeof(link_t) * alloc_links);
```

Wrong Size t Allocation\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1083
Status	New

The function alloc_images in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	780	780
Object	alloc_images	alloc_images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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);
```

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=1020042&projectid=20035&pathid=1152
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1034	1034
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1034.    bytes = alloc_headings * sizeof(int) * 2;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1153
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	741	741
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
741.      chapter_starts[1] = num_pages;
```

Integer Overflow\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1154
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	808	808
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1155
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	813	813
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 5:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1156
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	816	816
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1157
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
874.      page              = num_pages - 1;
```

Integer Overflow\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1158
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	876	876
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
876.      chapter_starts[0] = num_pages;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1159
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	882	882
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=1160
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1036	1036
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1036.    bytes += alloc_pages * sizeof(page_t);
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1161
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1048	1048
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1048.    bytes += num_outpages * sizeof(outpage_t);
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1162

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1318	1318
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1318.       chapter_outstarts[c] = num_outpages;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1163
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1358	1358
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1358.       chapter_outends[c] = num_outpages;
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1164
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3226 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3296	3296
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3296.       pages_object += num_links + 3;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1165
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3524 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3535	3535
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_names(FILE *out) /* I - Output file */

```
....
3535.     for (i = num_links, link = links; i > 0; i --, link ++)
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1166
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3524 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3576	3576
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_names(FILE *out) /* I - Output file */

```
....
3576.    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=1020042&projectid=20035&pathid=1167
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1049	1049
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1049.    bytes += alloc_links * sizeof(link_t);
```

Integer Overflow\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1168
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2812 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2904	2904
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2904.       entry             = num_objects + 3;
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1169
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2812 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2909	2909
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2909.       entry = num_objects + 2;
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1170
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3226 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3289	3289
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3289.    pages_object = num_objects + 1;
```

Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1171
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1050	1050
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1050.    bytes += alloc_objects * sizeof(int);
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1172
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1006 of michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.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-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	1012	1012
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_rlookup(const char *filename) /* I - Filename */

```
....
1012.    for (i = web_files, wc = web_cache; i > 0; i --, wc ++)
```

Integer Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1173
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1006 of michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.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-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	1012	1012
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_rlookup(const char *filename) /* I - Filename */

```
....
1012.    for (i = web_files, wc = web_cache; i > 0; i --, wc ++)
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1174
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1006 of michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.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-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	1012	1012
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_rlookup(const char *filename) /* I - Filename */

```
....
1012.    for (i = web_files, wc = web_cache; i > 0; i --, wc ++)
```

Integer Overflow\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1175
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1008 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	1014	1014
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_rlookup(const char *filename) /* I - Filename */

```
....
1014.    for (i = web_files, wc = web_cache; i > 0; i --, wc ++)
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1176
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1034	1034
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_debug_stats()

```
....
1034.    bytes = alloc_headings * sizeof(int) * 2;
```

Integer Overflow\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1177
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	741	741
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
741.      chapter_starts[1] = num_pages;
```

Integer Overflow\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1178
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	808	808
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1179
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	813	813
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1180
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	816	816
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1181
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
874.      page              = num_pages - 1;
```

Integer Overflow\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1182
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	876	876
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
876.      chapter_starts[0] = num_pages;
```

Integer Overflow\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1183
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	882	882
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1184
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1036	1036
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_debug_stats()

```
....
1036.    bytes += alloc_pages * sizeof(page_t);
```

Integer Overflow\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1185
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1048	1048
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_debug_stats()

```
....
1048.    bytes += num_outpages * sizeof(outpage_t);
```

Integer Overflow\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1186
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1318	1318
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1318.       chapter_outstarts[c] = num_outpages;
```

Integer Overflow\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1187
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1249 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1358	1358
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1358.       chapter_outends[c] = num_outpages;
```

Integer Overflow\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1188
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3224 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3294	3294
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3294.       pages_object += num_links + 3;
```

Integer Overflow\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1189
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3522 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3533	3533
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1190
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3522 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3574	3574
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1191
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1049	1049
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_debug_stats()

```
....
1049.    bytes += alloc_links * sizeof(link_t);
```

Integer Overflow\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1192
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2810 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2902	2902
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2902.       entry             = num_objects + 3;
```

Integer Overflow\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1193
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2810 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2907	2907
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2907.       entry = num_objects + 2;
```

Integer Overflow\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1194
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3224 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3287	3287
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3287.    pages_object = num_objects + 1;
```

Integer Overflow\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1195
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1050	1050
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_debug_stats()

```
....
1050.    bytes += alloc_objects * sizeof(int);
```

Integer Overflow\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1196
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1022 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	1034	1034
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_debug_stats()

```
....
1034.    bytes = alloc_headings * sizeof(int) * 2;
```

Integer Overflow\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1197
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	741	741
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
741.      chapter_starts[1] = num_pages;
```

Integer Overflow\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1198
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	808	808
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1199
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	813	813
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1200
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	816	816
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1201
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	874	874
Object	AssignExpr	AssignExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_export(tree_t *document, /* I - Document to export */

```
....
874.      page              = 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=1020042&projectid=20

	035&pathid=2567
Status	New

Calling free() (line 2094) on a variable that was not dynamically allocated (line 2094) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2179	2179
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method ps_write_page(FILE *out, /* I - Output file */

```
....
2179.       free(r);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2568
Status	New

Calling free() (line 2641) on a variable that was not dynamically allocated (line 2641) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2745	2745
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_page(FILE *out, /* I - Output file */

```
....
2745.       free(r);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2569

Status	New

Calling free() (line 2812) on a variable that was not dynamically allocated (line 2812) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2979	2979
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2979.         free(text);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2570
Status	New

Calling free() (line 3017) on a variable that was not dynamically allocated (line 3017) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3069	3069
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_files(FILE *out, // I - Output file

```
....
3069.           free(text);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2571
Status	New

Calling free() (line 3226) on a variable that was not dynamically allocated (line 3226) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3271	3271
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3271.           free(r);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2572
Status New

Calling free() (line 3596) on a variable that was not dynamically allocated (line 3596) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3792	3792
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3792.       free(temp);
```

MemoryFree on StackVariable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2573
Status New

Calling free() (line 4710) on a variable that was not dynamically allocated (line 4710) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4868	4868
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4868.           free(temp);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2574
Status New

Calling free() (line 4710) on a variable that was not dynamically allocated (line 4710) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	4949	4949
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4949.           free(temp);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2575
Status New

Calling free() (line 4710) on a variable that was not dynamically allocated (line 4710) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5234	5234
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5234.           free(linetype);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2576
Status New

Calling free() (line 4710) on a variable that was not dynamically allocated (line 4710) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5380	5380
Object	prev	prev

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5380.           free(prev);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2577
Status New

Calling free() (line 4710) on a variable that was not dynamically allocated (line 4710) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5402	5402
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5402.         free(linetype);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2578
Status New

Calling free() (line 5452) on a variable that was not dynamically allocated (line 5452) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5498	5498
Object	flat	flat

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5498.         free(flat);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2579
Status New

Calling free() (line 5452) on a variable that was not dynamically allocated (line 5452) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5643	5643
Object	start	start

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5643.         free(start);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2580
Status New

Calling free() (line 10271) on a variable that was not dynamically allocated (line 10271) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	10927	10927
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10927.            free(data);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2581
Status New

Calling free() (line 10271) on a variable that was not dynamically allocated (line 10271) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11020	11020
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
11020.            free(data);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2582
Status New

Calling free() (line 10271) on a variable that was not dynamically allocated (line 10271) in file michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11172	11172
Object	indices	indices

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
11172.      free(indices);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2583
Status New

Calling free() (line 2092) on a variable that was not dynamically allocated (line 2092) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2177	2177
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method ps_write_page(FILE *out, /* I - Output file */

```
....
2177.       free(r);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2584
Status New

Calling free() (line 2639) on a variable that was not dynamically allocated (line 2639) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2743	2743
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_page(FILE *out, /* I - Output file */

```
....
2743.       free(r);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2585
Status New

Calling free() (line 2810) on a variable that was not dynamically allocated (line 2810) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2977	2977
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2977.         free(text);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2586
Status New

Calling free() (line 3015) on a variable that was not dynamically allocated (line 3015) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3067	3067
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_files(FILE *out, // I - Output file

```
....
3067.           free(text);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2587
Status New

Calling free() (line 3224) on a variable that was not dynamically allocated (line 3224) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3269	3269
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3269.           free(r);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2588
Status New

Calling free() (line 3594) on a variable that was not dynamically allocated (line 3594) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3788	3788
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3788.       free(temp);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2589
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4844	4844
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4844.           free(temp);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2590
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	4925	4925
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4925.           free(temp);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2591
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5210	5210
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5210.           free(linetype);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2592
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5356	5356
Object	prev	prev

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5356.           free(prev);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2593
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5378	5378
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5378.         free(linetype);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2594
Status New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5474	5474
Object	flat	flat

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5474.         free(flat);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2595
Status New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5615	5615
Object	start	start

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5615.         free(start);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2596
Status New

Calling free() (line 10214) on a variable that was not dynamically allocated (line 10214) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	10870	10870
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10870.            free(data);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2597
Status New

Calling free() (line 10214) on a variable that was not dynamically allocated (line 10214) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	10963	10963
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10963.            free(data);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2598
Status New

Calling free() (line 10214) on a variable that was not dynamically allocated (line 10214) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11115	11115
Object	indices	indices

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
11115.      free(indices);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2599
Status New

Calling free() (line 2092) on a variable that was not dynamically allocated (line 2092) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	2177	2177
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method ps_write_page(FILE *out, /* I - Output file */

```
....
2177.       free(r);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2600
Status New

Calling free() (line 2639) on a variable that was not dynamically allocated (line 2639) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	2743	2743
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pdf_write_page(FILE *out, /* I - Output file */

```
....
2743.       free(r);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2601
Status New

Calling free() (line 2810) on a variable that was not dynamically allocated (line 2810) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	2977	2977
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pdf_write_contents(FILE *out, /* I - Output file */

```
....
2977.         free(text);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2602
Status New

Calling free() (line 3015) on a variable that was not dynamically allocated (line 3015) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	3067	3067
Object	text	text

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pdf_write_files(FILE *out, // I - Output file

```
....
3067.           free(text);
```

MemoryFree on StackVariable\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2603
Status New

Calling free() (line 3224) on a variable that was not dynamically allocated (line 3224) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	3269	3269
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3269.           free(r);
```

MemoryFree on StackVariable\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2604
Status New

Calling free() (line 3594) on a variable that was not dynamically allocated (line 3594) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	3788	3788
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method render_contents(tree_t *t, /* I - Tree to parse */

```
....
3788.       free(temp);
```

MemoryFree on StackVariable\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2605
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	4844	4844
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4844.           free(temp);
```

MemoryFree on StackVariable\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2606
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	4925	4925
Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
4925.           free(temp);
```

MemoryFree on StackVariable\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2607
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	5210	5210
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5210.           free(linetype);
```

MemoryFree on StackVariable\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2608
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	5356	5356
Object	prev	prev

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5356.           free(prev);
```

MemoryFree on StackVariable\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2609
Status New

Calling free() (line 4686) on a variable that was not dynamically allocated (line 4686) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	5378	5378
Object	linetype	linetype

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_paragraph(tree_t *t, /* I - Tree to parse */

```
....
5378.         free(linetype);
```

MemoryFree on StackVariable\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2610
Status New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	5474	5474
Object	flat	flat

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5474.         free(flat);
```

MemoryFree on StackVariable\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2611
Status New

Calling free() (line 5428) on a variable that was not dynamically allocated (line 5428) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	5615	5615
Object	start	start

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_pre(tree_t *t, /* I - Tree to parse */

```
....
5615.         free(start);
```

MemoryFree on StackVariable\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2612
Status New

Calling free() (line 10214) on a variable that was not dynamically allocated (line 10214) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	10870	10870
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10870.            free(data);
```

MemoryFree on StackVariable\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2613
Status New

Calling free() (line 10214) on a variable that was not dynamically allocated (line 10214) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	10963	10963
Object	data	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
10963.            free(data);
```

MemoryFree on StackVariable\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2614
Status New

Calling free() (line 10214) on a variable that was not dynamically allocated (line 10214) in file michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11115	11115
Object	indices	indices

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_image(FILE *out, /* I - Output file */

```
....
11115.      free(indices);
```

MemoryFree on StackVariable\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2615
Status New

Calling free() (line 2092) on a variable that was not dynamically allocated (line 2092) in file michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	2177	2177
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method ps_write_page(FILE *out, /* I - Output file */

```
....
2177.       free(r);
```

MemoryFree on StackVariable\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2616
Status New

Calling free() (line 2639) on a variable that was not dynamically allocated (line 2639) in file michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c may result with a crash.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	2743	2743
Object	r	r

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pdf_write_page(FILE *out, /* I - Output file */

```
....
2743.       free(r);
```

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=1020042&projectid=20

	035&pathid=971
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=972
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=973
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=974
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=975
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet

File Name mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c

Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=976
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet	
File Name	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c
Method	bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=977
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet	
File Name	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c
Method	bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=978
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c

Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=979
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=980
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=981
Status New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=982
Status New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.21.0-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.21.0-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.21.0-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.21.0-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.21.0-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=983
Status New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=984

Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.22.0-beta0-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=985
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.23.1-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.23.1-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.23.1-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.23.1-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.23.1-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 16:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=986
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.23.1-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.23.1-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.23.1-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.23.1-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.23.1-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=987
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.23.3-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.23.3-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.23.3-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.23.3-CVE-2024-6381-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.23.3-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=988
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.23.3-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.23.3-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.23.3-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.23.3-CVE-2024-6383-TP.c
Line	748	748
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.23.3-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
748.     cutoff /= base;
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=989
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.24.2-CVE-2024-6381-TP.c. In line 698, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.24.2-CVE-2024-6381-TP.c, at line 698.

	Source	Destination
File	mongodb@@mongo-c-driver-1.24.2-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.24.2-CVE-2024-6381-TP.c
Line	750	750
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.24.2-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
750.     cutoff /= base;
```

Divide By Zero\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=990
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.24.2-CVE-2024-6383-TP.c. In line 698, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.24.2-CVE-2024-6383-TP.c, at line 698.

	Source	Destination
File	mongodb@@mongo-c-driver-1.24.2-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.24.2-CVE-2024-6383-TP.c
Line	750	750
Object	base	base

Code Snippet

File Name mongodb@@mongo-c-driver-1.24.2-CVE-2024-6383-TP.c

Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
750.     cutoff /= base;
```

Divide By Zero\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=991
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.25.0-CVE-2024-6381-TP.c. In line 698, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.25.0-CVE-2024-6381-TP.c, at line 698.

	Source	Destination
File	mongodb@@mongo-c-driver-1.25.0-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.25.0-CVE-2024-6381-TP.c
Line	750	750
Object	base	base

Code Snippet	
File Name	mongodb@@mongo-c-driver-1.25.0-CVE-2024-6381-TP.c
Method	bson_ascii_strtoll (const char *s, char **e, int base)

```
....
750.     cutoff /= base;
```

Divide By Zero\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=992
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.25.0-CVE-2024-6383-TP.c. In line 698, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.25.0-CVE-2024-6383-TP.c, at line 698.

	Source	Destination
File	mongodb@@mongo-c-driver-1.25.0-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.25.0-CVE-2024-6383-TP.c
Line	750	750
Object	base	base

Code Snippet	
File Name	mongodb@@mongo-c-driver-1.25.0-CVE-2024-6383-TP.c
Method	bson_ascii_strtoll (const char *s, char **e, int base)

```
....
750.     cutoff /= base;
```

Divide By Zero\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=993
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.26.0-CVE-2024-6381-TP.c. In line 697, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.26.0-CVE-2024-6381-TP.c, at line 697.

	Source	Destination
File	mongodb@@mongo-c-driver-1.26.0-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.26.0-CVE-2024-6381-TP.c

Line	749	749
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.26.0-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
749.     cutoff /= base;
```

Divide By Zero\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=994
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.26.0-CVE-2024-6383-TP.c. In line 697, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.26.0-CVE-2024-6383-TP.c, at line 697.

	Source	Destination
File	mongodb@@mongo-c-driver-1.26.0-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.26.0-CVE-2024-6383-TP.c
Line	749	749
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.26.0-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
749.     cutoff /= base;
```

Divide By Zero\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=995
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6753	6753
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=996
Status New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c, at line 6321.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6935	6935
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=997
Status New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.16-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-v1.9.16-CVE-2021-23180-FP.c, at line 350.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	577	577
Object	total	total

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
577.        progress_update((100 * count / total) % 101);
```

Divide By Zero\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=998
Status New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.17-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-v1.9.17-CVE-2021-23180-FP.c, at line 350.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	577	577
Object	total	total

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
577.        progress_update((100 * count / total) % 101);
```

Divide By Zero\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=999
Status New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.18-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-v1.9.18-CVE-2021-23180-FP.c, at line 350.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	577	577
Object	total	total

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
577.        progress_update((100 * count / total) % 101);
```

Divide By Zero\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1000
Status New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c. In line 347, 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-v1.9.8-CVE-2021-23180-TP.c, at line 347.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	587	587
Object	total	total

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
587.        progress_update((100 * count / total) % 101);
```

Divide By Zero\Path 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1001
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c. In line 6293, 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-v1.9.8-CVE-2021-23206-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	6697	6697
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6697.    regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1002
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c. In line 6293, 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-v1.9.8-CVE-2021-23206-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	6879	6879
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6879.        regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1003
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c. In line 6293, 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-v1.9.8-CVE-2022-28085-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	6697	6697
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6697.     regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1004
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c. In line 6293, 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-v1.9.8-CVE-2022-28085-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	6879	6879
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6879.        regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1005
Status	New

The application performs an illegal operation in file_find_check, in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23180-TP.c, at line 348.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	575	575
Object	total	total

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1006
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c. In line 6293, 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-v1.9.9-CVE-2021-23206-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	6697	6697
Object	num_cols	num_cols

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6697.    regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1007
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c. In line 6293, 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-v1.9.9-CVE-2021-23206-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	6879	6879
Object	num_cols	num_cols

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6879.        regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1008
Status	New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c. In line 6293, 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-v1.9.9-CVE-2022-28085-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c

Line	6697	6697
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6697.    regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1009
Status New

The application performs an illegal operation in parse_table, in michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c. In line 6293, 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-v1.9.9-CVE-2022-28085-TP.c, at line 6293.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	6879	6879
Object	num_cols	num_cols

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6879.        regular_width = (width - actual_width) / table.num_cols;
```

Divide By Zero\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1010
Status New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1011
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.0-beta2-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1012
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.1-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1013
Status New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.1-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=1014
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.4-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1015
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.4-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 46:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1016
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.6-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1017
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.17.6-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1018
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.19.1-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1019
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c	mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.19.1-CVE-2024-6383-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

Divide By Zero\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=1020
Status	New

The application performs an illegal operation in bson_ascii_strtoll, in mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c. In line 696, the program attempts to divide by base, 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 base in bson_ascii_strtoll of mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c, at line 696.

	Source	Destination
File	mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c	mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c
Line	747	747
Object	base	base

Code Snippet
File Name mongodb@@mongo-c-driver-1.21.0-CVE-2024-6381-TP.c
Method bson_ascii_strtoll (const char *s, char **e, int base)

```
....
747.     cutlim = (int) (cutoff % base);
```

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=1020042&projectid=20035&pathid=2524
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11747	11779
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2525
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11736	11809
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2526
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11736	11832
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2527
Status New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11736	11833
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=2528
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c at line 11300.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11736	11803
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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);
```

Inadequate Encryption Strength\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2529
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11690	11722
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11690.      if ((i = strlen(OwnerPassword)) < 32)
....
11722.        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=1020042&projectid=20035&pathid=2530
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11679	11752
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11752.          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=1020042&projectid=20035&pathid=2531
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11679	11775
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11775.        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=1020042&projectid=20035&pathid=2532
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11679	11776
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.          if ((i = strlen(UserPassword)) < 32)
....
11776.          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=1020042&projectid=20035&pathid=2533
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11679	11746
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11746.            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=1020042&projectid=20035&pathid=2534
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11690	11722
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11690.      if ((i = strlen(OwnerPassword)) < 32)
....
11722.        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=1020042&projectid=20035&pathid=2535
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11679	11752
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11752.          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=1020042&projectid=20035&pathid=2536
Status New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11679	11775
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11775.        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=1020042&projectid=20035&pathid=2537
Status New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11679	11776

Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11776.        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=1020042&projectid=20035&pathid=2538
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11679	11746
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11746.            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=1020042&projectid=20035&pathid=2539
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-	michaelrsweet@@htmldoc-v1.9.9-CVE-

	2021-23206-TP.c	2021-23206-TP.c
Line	11690	11722
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11690.      if ((i = strlen(OwnerPassword)) < 32)
....
11722.        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=1020042&projectid=20035&pathid=2540
Status New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11679	11752
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11752.          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=1020042&projectid=20035&pathid=2541
Status New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11679	11775
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.          if ((i = strlen(UserPassword)) < 32)
....
11775.          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=1020042&projectid=20035&pathid=2542
Status New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11679	11776
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.          if ((i = strlen(UserPassword)) < 32)
....
11776.          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=1020042&projectid=20035&pathid=2543
Status New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11679	11746
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11746.            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=1020042&projectid=20035&pathid=2544
Status New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c, to protect sensitive personal information OwnerPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11690	11722
Object	OwnerPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11690.      if ((i = strlen(OwnerPassword)) < 32)
....
11722.        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=1020042&projectid=20

	035&pathid=2545
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11679	11752
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11752.          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=1020042&projectid=20035&pathid=2546
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11679	11775
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11775.        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=1020042&projectid=20035&pathid=2547
Status	New

The application uses a weak cryptographic algorithm, _cupsMD5Append at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11679	11776
Object	UserPassword	_cupsMD5Append

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11776.        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=1020042&projectid=20035&pathid=2548
Status	New

The application uses a weak cryptographic algorithm, rc4_encrypt at line 11243 of michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c, to protect sensitive personal information UserPassword, from michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c at line 11243.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11679	11746
Object	UserPassword	rc4_encrypt

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11679.        if ((i = strlen(UserPassword)) < 32)
....
11746.            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=1020042&projectid=20035&pathid=2505
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	669	679
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_flush_cache(void)

```
....
669.          free(images[i]->mask);
....
679.        free(images);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2506
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	672	679
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_flush_cache(void)

```
....
672.         free(images[i]->pixels);
....
679.       free(images);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2507
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-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=1020042&projectid=20035&pathid=2508
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-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=1020042&projectid=20035&pathid=2509
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.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=1020042&projectid=20035&pathid=2510
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.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=1020042&projectid=20035&pathid=2511
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.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=1020042&projectid=20035&pathid=2512
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.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=1020042&projectid=20035&pathid=2513
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Method image_flush_cache(void)

```
....
640.         free(images[i]->mask);
....
650.       free(images);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2514
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Method image_flush_cache(void)

```
....
643.         free(images[i]->pixels);
....
650.       free(images);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2515
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Method image_flush_cache(void)

```
....
640.         free(images[i]->mask);
....
650.       free(images);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2516
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Method image_flush_cache(void)

```
....
643.         free(images[i]->pixels);
....
650.       free(images);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2517
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Method image_flush_cache(void)

```
....
640.         free(images[i]->mask);
....
650.       free(images);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2518
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Method image_flush_cache(void)

```
....
643.         free(images[i]->pixels);
....
650.       free(images);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2519
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Method image_flush_cache(void)

```
....
640.         free(images[i]->mask);
....
650.       free(images);
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2520
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Method image_flush_cache(void)

```
....
643.         free(images[i]->pixels);
....
650.       free(images);
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2521
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Line	640	650
Object	mask	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Method image_flush_cache(void)

```
....
640.         free(images[i]->mask);
....
650.       free(images);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2522
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Line	643	650
Object	pixels	images

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Method image_flush_cache(void)

```
....
643.         free(images[i]->pixels);
....
650.       free(images);
```

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=1020042&projectid=20035&pathid=3220
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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=1020042&projectid=20035&pathid=3221
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-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=1020042&projectid=20035&pathid=3222
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-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=1020042&projectid=20035&pathid=3223
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c

Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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=1020042&projectid=20035&pathid=3224
Status	New

The variable 16 at line 238 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	238	238
Object	16	encrypt_key

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method static uchar encrypt_key[16];

```
....
238.  static uchar            encrypt_key[16];
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3351
Status	New

The variable declared in tmp at mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c in line 7212 is not initialized when it is used by tmp at mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c in line 7212.

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	7214	7219
Object	tmp	tmp

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Method int mp_shrink (mp_int * a)

```
....
7214.    mp_digit *tmp;
....
7219.      a->dp     = tmp;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3352
Status	New

The variable declared in temp at michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c in line 435 is not initialized when it is used by temp at michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c in line 435.

	Source	Destination
File	michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c	michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c
Line	438	450
Object	temp	temp

Code Snippet
File Name michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c
Method _pdfioDictGetValue(pdfio_dict_t *dict, // I - Dictionary

```
....
438.    _pdfio_pair_t   temp,              // Search key
....
450.    temp.key = key;
```

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=1020042&projectid=20035&pathid=1151
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 6099 of mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	6130	6130
Object	AssignExpr	AssignExpr

Code Snippet

File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c

Method int mp_prime_random_ex(mp_int *a, int t, int size, int flags, ltm_prime_callback cb, void *dat)

```
....
6130.         maskOR_msb       |= 0x80 >> ((9 - size) & 7);
```

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=1020042&projectid=20035&pathid=2523
Status	New

Method *pwd; at line 288 of mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination

File	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	288	288
Object	pwd	pwd

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method struct passwd *pwd;

```
....
288.  struct passwd *pwd;
```

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=1020042&projectid=20035&pathid=3489
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11676	11676
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3490

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12482	12482
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3491
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12502	12502
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3492
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Line	12509	12509
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3493
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12519	12519
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3494
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12533	12533
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3495
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12541	12541
Object	fgets	fgets

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3496
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12566	12566
Object	fgets	fgets

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-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 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3497
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12611	12611
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3498
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11619	11619
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11619.      while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3499
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12422	12422
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12422.      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=1020042&projectid=20035&pathid=3500
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12442	12442
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12442.      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=1020042&projectid=20035&pathid=3501
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12449	12449

Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12449.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3502
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12459	12459
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12459.      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=1020042&projectid=20035&pathid=3503
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12473	12473
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12473.      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=1020042&projectid=20035&pathid=3504
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12481	12481
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12481.      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=1020042&projectid=20035&pathid=3505
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12506	12506
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12506.      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=1020042&projectid=20035&pathid=3506
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12551	12551
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12551.      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=1020042&projectid=20035&pathid=3507
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11619	11619
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11619.      while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3508
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12422	12422
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12422.      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=1020042&projectid=20035&pathid=3509
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12442	12442
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12442.      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=1020042&projectid=20035&pathid=3510
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12449	12449

Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12449.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3511
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12459	12459
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12459.      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=1020042&projectid=20035&pathid=3512
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12473	12473
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12473.      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=1020042&projectid=20035&pathid=3513
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12481	12481
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12481.      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=1020042&projectid=20035&pathid=3514
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12506	12506
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12506.      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=1020042&projectid=20035&pathid=3515
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12551	12551
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12551.      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=1020042&projectid=20035&pathid=3516
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11619	11619
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11619.      while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3517
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12422	12422
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12422.      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=1020042&projectid=20035&pathid=3518
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12442	12442
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12442.      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=1020042&projectid=20035&pathid=3519
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12449	12449

Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12449.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3520
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12459	12459
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12459.      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=1020042&projectid=20035&pathid=3521
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12473	12473
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12473.      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=1020042&projectid=20035&pathid=3522
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12481	12481
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12481.      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=1020042&projectid=20035&pathid=3523
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12506	12506
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12506.      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=1020042&projectid=20035&pathid=3524
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12551	12551
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12551.      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=1020042&projectid=20035&pathid=3525
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11619	11619
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11619.      while (fgets(temp, sizeof(temp), prolog) != NULL)
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3526
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12422	12422
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12422.      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=1020042&projectid=20035&pathid=3527
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12442	12442
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12442.      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=1020042&projectid=20035&pathid=3528
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12449	12449

Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12449.      while (fgets(line, sizeof(line), fp) != NULL)
```

Improper Resource Access Authorization\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3529
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12459	12459
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12459.      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=1020042&projectid=20035&pathid=3530
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12473	12473
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12473.      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=1020042&projectid=20035&pathid=3531
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12481	12481
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12481.      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=1020042&projectid=20035&pathid=3532
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12506	12506
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12506.      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=1020042&projectid=20035&pathid=3533
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	12551	12551
Object	fgets	fgets

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12551.      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=1020042&projectid=20035&pathid=3534
Status	New

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	3055	3055
Object	fgetc	fgetc

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Method int mp_fread(mp_int *a, int radix, FILE *stream)

```
....
3055.      ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3535
Status	New

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	3058	3058
Object	fgetc	fgetc

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Method int mp_fread(mp_int *a, int radix, FILE *stream)

```
....
3058.         ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3536
Status New

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	3082	3082
Object	fgetc	fgetc

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Method int mp_fread(mp_int *a, int radix, FILE *stream)

```
....
3082.         ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3537
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11676	11676

Object	temp	temp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3538
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12482	12482
Object	line	line

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12482.      while (fgets(line, sizeof(line), fp) != 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=1020042&projectid=20035&pathid=2900
Status New

The size of the buffer used by image_load_bmp in width, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	965
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    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=1020042&projectid=20035&pathid=2901
Status New

The size of the buffer used by image_load_bmp in width, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	965
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2902
Status	New

The size of the buffer used by image_load_bmp in width, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	965
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2903
Status	New

The size of the buffer used by image_load_bmp in width, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	965
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    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=1020042&projectid=20035&pathid=2904
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	965
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2905
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	965
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2906
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	965
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    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=1020042&projectid=20035&pathid=2907
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	965
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    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=1020042&projectid=20035&pathid=2908
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	965
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    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=1020042&projectid=20035&pathid=2909
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	965
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2910
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	965
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    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=1020042&projectid=20035&pathid=2911
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	965
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method	image_load_bmp(image_t *img, /* I - Image to load into */

```
....
965.    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=1020042&projectid=20035&pathid=2912
Status	New

The size of the buffer used by image_load_bmp in long, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	965
Object	getc	long

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2913
Status	New

The size of the buffer used by image_load_bmp in long, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	965
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2914
Status	New

The size of the buffer used by image_load_bmp in long, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	965
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2915
Status	New

The size of the buffer used by image_load_bmp in long, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	965
Object	getc	long

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2916
Status	New

The size of the buffer used by image_load_bmp in height, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1936	965
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1936.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2917
Status	New

The size of the buffer used by image_load_bmp in height, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1937	965
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1937.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2918
Status	New

The size of the buffer used by image_load_bmp in height, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1938	965
Object	getc	height

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
1938.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2919
Status	New

The size of the buffer used by image_load_bmp in height, at line 895 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_long passes to getc, at line 1932 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1939	965

Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1939.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

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

```
....
965.    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=1020042&projectid=20035&pathid=2920
Status New

The size of the buffer used by image_load_gif in height, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 getc, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1310	1373
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1310.            buf[0] = (uchar)getc(fp);
....
1373.            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=1020042&projectid=20

	035&pathid=2921
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 getc, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1310	1373
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1310.            buf[0] = (uchar)getc(fp);
....
1373.            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=1020042&projectid=20035&pathid=2922
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 getc, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1310	1373
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1310.            buf[0] = (uchar)getc(fp);
....
1373.            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=1020042&projectid=20035&pathid=2923
Status	New

The size of the buffer used by image_load_gif in long, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 getc, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1310	1373
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1310.            buf[0] = (uchar)getc(fp);
....
1373.            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=1020042&projectid=20035&pathid=2924
Status	New

The size of the buffer used by image_load_gif in width, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 getc, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1310	1373
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1310.            buf[0] = (uchar)getc(fp);
....
1373.            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=1020042&projectid=20035&pathid=2925
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2926
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	925
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2927
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	925
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2928
Status	New

The size of the buffer used by image_load_bmp in width, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	925
Object	getc	width

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2929
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	925
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2930
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	925
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2931
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 33:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2932
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2933
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.8-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 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2934
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	925
Object	getc	BinaryExpr

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method	read_long(FILE *fp) /* I - File to read from */

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name	michaelrsweet@@htmldoc-v1.9.8-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 36:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2935
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2936
Status	New

The size of the buffer used by image_load_bmp in BinaryExpr, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	925
Object	getc	BinaryExpr

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2937
Status New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 39:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2938
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	925
Object	getc	long

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2939
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2940
Status	New

The size of the buffer used by image_load_bmp in long, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	925
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2941
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1841	925
Object	getc	height

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1841.    b0 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2942
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1842	925
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1842.    b1 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2943
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1843	925
Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method read_long(FILE *fp) /* I - File to read from */

```
....
1843.    b2 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2944
Status	New

The size of the buffer used by image_load_bmp in height, at line 862 of michaelrsweet@@htmldoc-v1.9.8-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 1837 of michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1844	925
Object	getc	height

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

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

```
....
1844.    b3 = (uchar)getc(fp);
```

File Name michaelrsweet@@htmldoc-v1.9.8-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 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2945
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1267	1326

Object	getc	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2946
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2947
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2948
Status New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 50:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2949
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1267	1326
Object	getc	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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));
```

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=1020042&projectid=20035&pathid=5939
Status	New

The render_table_row method calls the snprintf function, at line 5713 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	5831	5831
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_table_row(hdtable_t &table,

```
....
5831.           snprintf(table_text, sizeof(table_text), "cell=%p
[%d,%d]",
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5940
Status	New

The parse_table method calls the snprintf function, at line 6321 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	7032	7032
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
7032.       snprintf(table_text, sizeof(table_text), "t=%p", (void *)t);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5941
Status	New

The parse_list method calls the snprintf function, at line 7239 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	7320	7320

Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_list(tree_t *t, /* I - Tree to parse */

```
....
7320.          snprintf((char *)number, sizeof(number), "%c ",
list_types[t->indent]);
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5942
Status New

The open_file method calls the snprintf function, at line 9798 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9806	9806
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9806.        snprintf(filename, sizeof(filename), "%s/cover.ps",
OutputPath);
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5943
Status New

The open_file method calls the snprintf function, at line 9798 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-	michaelrsweet@@htmldoc-v1.9.13-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	9808	9808
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9808.         snprintf(filename, sizeof(filename), "%s/contents.ps",
OutputPath);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5944
Status	New

The open_file method calls the snprintf function, at line 9798 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9810	9810
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9810.         snprintf(filename, sizeof(filename), "%s/doc%d.ps",
OutputPath, chapter);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5945
Status	New

The open_file method calls the snprintf function, at line 9798 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9816	9816
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9816.      snprintf(filename, sizeof(filename), "%s/doc.pdf",
OutputPath);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5946
Status New

The set_font method calls the snprintf function, at line 9872 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9890	9890
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method set_font(FILE *out, /* I - File to write to */

```
....
9890.    snprintf(sizes, sizeof(sizes), "%.1f", size);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5947
Status New

The set_pos method calls the snprintf function, at line 9923 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9941	9941
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method set_pos(FILE *out, /* I - File to write to */

```
....
9941.       snprintf(xs, sizeof(xs), "%.3f", x);
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5948
Status New

The set_pos method calls the snprintf function, at line 9923 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9942	9942
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method set_pos(FILE *out, /* I - File to write to */

```
....
9942.       snprintf(ys, sizeof(ys), "%.3f", y);
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5949
Status New

The set_pos method calls the snprintf function, at line 9923 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9946	9946
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method set_pos(FILE *out, /* I - File to write to */

```
....
9946.       snprintf(xs, sizeof(xs), "%.3f", x - render_startx);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5950
Status New

The set_pos method calls the snprintf function, at line 9923 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9947	9947
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method set_pos(FILE *out, /* I - File to write to */

```
....
9947.       snprintf(ys, sizeof(ys), "%.3f", y - render_y);
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5951

Status	New

The write_prolog method calls the snprintf function, at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11673	11673
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11673.        snprintf(temp, sizeof(temp), "%s/data/prolog.ps",
_htmlData);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5952
Status	New

The write_prolog method calls the snprintf function, at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11923	11923
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11923.      snprintf(temp, sizeof(temp),
"D:%04d%02d%02d%02d%02d%02d+0000",
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5953
Status	New

The write_prolog method calls the snprintf function, at line 11300 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11937	11937
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11937.          snprintf(temp, sizeof(temp), "%s, %s", author,
copyright);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5954
Status	New

The write_type1 method calls the snprintf function, at line 12403 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12457	12457
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12457.    snprintf(filename, sizeof(filename), "%s/fonts/%s.pfa",
_htmlData,
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5955
Status	New

The write_type1 method calls the snprintf function, at line 12403 of michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12579	12579
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12579.      snprintf(filename, sizeof(filename), "%s/fonts/%s.afm",
_htmlData,
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5956
Status	New

The httpAddrString method calls the snprintf function, at line 499 of michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-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-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	533	533
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Method httpAddrString(const http_addr_t *addr, /* I - Address to convert */

```
....
533.      snprintf(s, (size_t)slen, "%d.%d.%d.%d", (temp >> 24) & 255,
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5957
Status	New

The httpAddrString method calls the snprintf function, at line 499 of michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-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-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	636	636
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Method httpAddrString(const http_addr_t *addr, /* I - Address to convert */

```
....
636.      snprintf(s, (size_t)slen, "[v1.%s]", temps);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5958
Status	New

The httpGetHostname method calls the snprintf function, at line 819 of michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-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-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	871	871
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c

Method	httpGetHostname(http_t *http, /* I - HTTP connection or NULL */

```
....
871.          snprintf(s, (size_t)slen, "%s.local.", localStr);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5959
Status	New

The file_temp method calls the snprintf function, at line 1060 of michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	1117	1117
Object	snprintf	snprintf

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method	file_temp(char *name, /* O - Filename */

```
....
1117.    snprintf(name, (size_t)len, TEMPLATE, tmpdir, (long)getpid(),
(int)web_files);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5960
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	159	159
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
159.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5961
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	186	186
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
186.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5962
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	197	197

Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
197.      snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)web_files);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5963
Status	New

The file_localize method calls the snprintf function, at line 833 of michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	874	874
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
874.      snprintf(temp, sizeof(temp), "%s/%s", cwd, newslash);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5964
Status	New

The image_copy method calls the snprintf function, at line 551 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

Line	571	571
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
571.      snprintf(dest, sizeof(dest), "%s/%s", destpath,
file_basename(src));
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5965
Status	New

The httpAddrString method calls the snprintf function, at line 499 of michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-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-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	533	533
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Method httpAddrString(const http_addr_t *addr, /* I - Address to convert */

```
....
533.      snprintf(s, (size_t)slen, "%d.%d.%d.%d", (temp >> 24) & 255,
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5966
Status	New

The httpAddrString method calls the snprintf function, at line 499 of michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-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-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	636	636
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Method httpAddrString(const http_addr_t *addr, /* I - Address to convert */

```
....
636.      snprintf(s, (size_t)slen, "[v1.%s]", temps);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5967
Status	New

The httpGetHostname method calls the snprintf function, at line 819 of michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-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-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	871	871
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Method httpGetHostname(http_t *http, /* I - HTTP connection or NULL */

```
....
871.          snprintf(s, (size_t)slen, "%s.local.", localStr);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5968
Status	New

The file_temp method calls the snprintf function, at line 1060 of michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	1117	1117
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_temp(char *name, /* O - Filename */

```
....
1117.    snprintf(name, (size_t)len, TEMPLATE, tmpdir, (long)getpid(),
(int)web_files);
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5969
Status New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	159	159
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
159.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5970
Status New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	186	186
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
186.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5971
Status New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	197	197
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
197.      snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)web_files);
```

Unchecked Return Value\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=5972
Status	New

The file_localize method calls the snprintf function, at line 833 of michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	874	874
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
874.      snprintf(temp, sizeof(temp), "%s/%s", cwd, newslash);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5973
Status	New

The file_temp method calls the snprintf function, at line 1060 of michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	1117	1117
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_temp(char *name, /* O - Filename */

```
....
1117.    snprintf(name, (size_t)len, TEMPLATE, tmpdir, (long)getpid(),
(int)web_files);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5974
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	159	159
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
159.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5975
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	186	186
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
186.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5976
Status	New

The file_cleanup method calls the snprintf function, at line 117 of michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	197	197
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_cleanup(void)

```
....
197.      snprintf(filename, sizeof(filename), 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=1020042&projectid=20035&pathid=5977
Status	New

The file_localize method calls the snprintf function, at line 833 of michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-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	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	874	874
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
874.      snprintf(temp, sizeof(temp), "%s/%s", cwd, newslash);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5978
Status	New

The file_temp method calls the snprintf function, at line 1055 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	1112	1112
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_temp(char *name, /* O - Filename */

```
....
1112.    snprintf(name, (size_t)len, TEMPLATE, tmpdir, (long)getpid(),
(int)web_files);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5979
Status	New

The file_cleanup method calls the snprintf function, at line 116 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	158	158
Object	snprintf	snprintf

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method	file_cleanup(void)

```
....
158.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5980
Status	New

The file_cleanup method calls the snprintf function, at line 116 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	185	185
Object	snprintf	snprintf

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method	file_cleanup(void)

```
....
185.        snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)(i + 1));
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5981
Status	New

The file_cleanup method calls the snprintf function, at line 116 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	196	196

Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_cleanup(void)

```
....
196.      snprintf(filename, sizeof(filename), TEMPLATE, tmpdir,
(long)getpid(), (int)web_files);
```

Unchecked Return Value\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5982
Status New

The file_find_check method calls the snprintf function, at line 347 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	473	473
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_find_check(const char *filename) /* I - File or URL */

```
....
473.          snprintf(connpath, sizeof(connpath), "%s://%s:%d%s",
scheme,
```

Unchecked Return Value\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5983
Status New

The file_localize method calls the snprintf function, at line 837 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-	michaelrsweet@@htmldoc-v1.9.8-CVE-

	2021-23180-TP.c	2021-23180-TP.c
Line	878	878
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
878.      snprintf(temp, sizeof(temp), "%s/%s", cwd, newslash);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5984
Status	New

The image_copy method calls the snprintf function, at line 522 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	542	542
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5985
Status	New

The render_table_row method calls the snprintf function, at line 5685 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	5803	5803
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method render_table_row(hdtable_t &table,

```
....
5803.           snprintf(table_text, sizeof(table_text), "cell=%p
[%d,%d]",
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5986
Status	New

The parse_table method calls the snprintf function, at line 6293 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	6976	6976
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6976.       snprintf(table_text, sizeof(table_text), "t=%p", (void *)t);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5987
Status	New

The parse_list method calls the snprintf function, at line 7183 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	7264	7264
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_list(tree_t *t, /* I - Tree to parse */

```
....
7264.          snprintf((char *)number, sizeof(number), "%c ",
list_types[t->indent]);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5988
Status	New

The open_file method calls the snprintf function, at line 9741 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	9749	9749
Object	snprintf	snprintf

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9749.        snprintf(filename, sizeof(filename), "%s/cover.ps",
OutputPath);
```

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=1020042&projectid=20035&pathid=2651
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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));
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2652
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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));
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2653
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 1497 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 1497.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1539	1784
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_prepare_heading(int page, // I - Page number

```
....
1539.      temp = NULL;
....
1784.        get_color(_htmlTextColor, temp->data.text.rgb);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2654
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 3226 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 3226.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	3256	3262
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3256.         for (r = p->start, x = 0.0f, y = 0.0f, rlast = NULL, rprev
= NULL;
....
3262.              rlast != NULL && strcmp((const char *)rlast-
>data.link,
```

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2655
Status New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 6321 is not initialized when it is used by cells at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 5713.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6396	6043
Object	null	cells

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6396.     cells = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method render_table_row(hdtable_t &table,

```
....
6043.         DEBUG_printf(("row = %d, col = %d, valign = %d, rowspans =
%d, cell_height = %.1f, span_heights = %.1f, delta_y = %.1f\n", row,
col, cells[row][col]->valignment, table.row_spans[col],
table.cell_height[col], table.span_heights[col], delta_y));
```

NULL Pointer Dereference\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2656

Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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));
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2657
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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));
```

NULL Pointer Dereference\Path 8:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2658
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 1495 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 1495.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1537	1782
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_prepare_heading(int page, // I - Page number

```
....
1537.       temp = NULL;
....
1782.         get_color(_htmlTextColor, temp->data.text.rgb);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2659
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 3224 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 3224.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	3254	3260
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3254.         for (r = p->start, x = 0.0f, y = 0.0f, rlast = NULL, rprev
= NULL;
....
3260.              rlast != NULL && strcmp((const char *)rlast-
>data.link,
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2660
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 6293 is not initialized when it is used by cells at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 5685.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	6368	6015
Object	null	cells

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c

Method parse_table(tree_t *t, // I - Tree to parse

```
....
6368.     cells = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c

Method render_table_row(hdtable_t &table,

```
....
6015.         DEBUG_printf(("row = %d, col = %d, valign = %d, rowspans =
%d, cell_height = %.1f, span_heights = %.1f, delta_y = %.1f\n", row,
col, cells[row][col]->valignment, table.row_spans[col],
table.cell_height[col], table.span_heights[col], delta_y));
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2661
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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));
```

NULL Pointer Dereference\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2662
Status New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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));
```

NULL Pointer Dereference\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2663
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 1495 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 1495.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	1537	1782
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_prepare_heading(int page, // I - Page number

```
....
1537.       temp = NULL;
....
1782.         get_color(_htmlTextColor, temp->data.text.rgb);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2664
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 3224 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 3224.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	3254	3260
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3254.         for (r = p->start, x = 0.0f, y = 0.0f, rlast = NULL, rprev
= NULL;
....
3260.              rlast != NULL && strcmp((const char *)rlast-
>data.link,
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2665
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 6293 is not initialized when it is used by cells at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 5685.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	6368	6015
Object	null	cells

Code Snippet

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c

Method parse_table(tree_t *t, // I - Tree to parse

```
....
6368.     cells = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c

Method render_table_row(hdtable_t &table,

```
....
6015.         DEBUG_printf(("row = %d, col = %d, valign = %d, rowspans =
%d, cell_height = %.1f, span_heights = %.1f, delta_y = %.1f\n", row,
col, cells[row][col]->valignment, table.row_spans[col],
table.cell_height[col], table.span_heights[col], delta_y));
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2666
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	523	726

Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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));
```

NULL Pointer Dereference\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2667
Status New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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));
```

NULL Pointer Dereference\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2668
Status New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 1495 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 1495.

	Source	Destination

File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	1537	1782
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pspdf_prepare_heading(int page, // I - Page number

```
....
1537.       temp = NULL;
....
1782.         get_color(_htmlTextColor, temp->data.text.rgb);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2669
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 3224 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 3224.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	3254	3260
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3254.         for (r = p->start, x = 0.0f, y = 0.0f, rlast = NULL, rprev
= NULL;
....
3260.              rlast != NULL && strcmp((const char *)rlast-
>data.link,
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2670
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 6293 is not initialized when it is used by cells at michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c in line 5685.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	6368	6015
Object	null	cells

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6368.     cells = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method render_table_row(hdtable_t &table,

```
....
6015.         DEBUG_printf(("row = %d, col = %d, valign = %d, rowspans =
%d, cell_height = %.1f, span_heights = %.1f, delta_y = %.1f\n", row,
col, cells[row][col]->valignment, table.row_spans[col],
table.cell_height[col], table.span_heights[col], delta_y));
```

NULL Pointer Dereference\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2671
Status New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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));
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2672
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 373 is not initialized when it is used by pages at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 373.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	523	726
Object	null	pages

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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));
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2673
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 1495 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 1495.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	1537	1782
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method pspdf_prepare_heading(int page, // I - Page number

```
....
1537.       temp = NULL;
....
1782.         get_color(_htmlTextColor, temp->data.text.rgb);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2674
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 3224 is not initialized when it is used by data at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 3224.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	3254	3260
Object	null	data

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method pdf_write_links(FILE *out) /* I - Output file */

```
....
3254.         for (r = p->start, x = 0.0f, y = 0.0f, rlast = NULL, rprev
= NULL;
....
3260.              rlast != NULL && strcmp((const char *)rlast-
>data.link,
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2675
Status	New

The variable declared in null at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 6293 is not initialized when it is used by cells at michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c in line 5685.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-	michaelrsweet@@htmldoc-v1.9.9-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	6368	6015
Object	null	cells

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6368.    cells = NULL;
```

File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c

Method render_table_row(hdtable_t &table,

```
....
6015.        DEBUG_printf(("row = %d, col = %d, valign = %d, rowspans =
%d, cell_height = %.1f, span_heights = %.1f, delta_y = %.1f\n", row,
col, cells[row][col]->valignment, table.row_spans[col],
table.cell_height[col], table.span_heights[col], delta_y));
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2676
Status	New

The variable declared in null at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	171
Object	null	current_palette

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
171.                          putc(current_palette[i].r, ftga);
```

NULL Pointer Dereference\Path 27:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2677
Status	New

The variable declared in null at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	170
Object	null	current_palette

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
170.                          putc(current_palette[i].g, ftga);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2678
Status	New

The variable declared in null at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11 is not initialized when it is used by current_palette at miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c in line 11.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	14	169
Object	null	current_palette

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
14.   struct ngiflib_rgb * current_palette = NULL;
....
169.                          putc(current_palette[i].b, ftga);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2679
Status	New

The variable declared in null at mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c in line 504 is not initialized when it is used by registry at mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c in line 463.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	506	488
Object	null	registry

Code Snippet

File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c

Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
506.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c

Method int convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
488.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2680
Status	New

The variable declared in null at mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c in line 504 is not initialized when it is used by registry at mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c in line 463.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	506	488
Object	null	registry

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
506.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c

Method int convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
488.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2681
Status	New

The variable declared in null at mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c in line 504 is not initialized when it is used by registry at mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c in line 463.

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	506	488
Object	null	registry

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
506.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c

Method int convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
488.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2682
Status	New

The variable declared in null at mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c in line 504 is not initialized when it is used by registry at mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c in line 463.

	Source	Destination
File	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Line	506	488
Object	null	registry

Code Snippet

File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c

Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
506.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c

Method int convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
488.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2683
Status	New

The variable declared in null at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 502 is not initialized when it is used by registry at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 461.

	Source	Destination
File	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Line	504	486
Object	null	registry

Code Snippet

File Name mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
504.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Method int convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
486.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2684
Status New

The variable declared in null at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 2835 is not initialized when it is used by options at mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c in line 502.

	Source	Destination
File	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Line	2843	531
Object	null	options

Code Snippet
File Name mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Method static PyObject* _cbson_decode_all(PyObject* self, PyObject* args) {

```
....
2843.      PyObject* options_obj = NULL;
```

File Name mongodb@@mongo-python-driver-3.13.0-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
531.      Py_INCREF(options->options_obj);
```

NULL Pointer Dereference\Path 35:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2685
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 465 is not initialized when it is used by registry at mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c in line 424.

	Source	Destination
File	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Line	467	449
Object	null	registry

Code Snippet
File Name mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
467.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-4.1.0-CVE-2024-21506-TP.c
Method int convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
449.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2686
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 462 is not initialized when it is used by registry at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 421.

	Source	Destination
File	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Line	464	446
Object	null	registry

Code Snippet
File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
464.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c

Method int cbson_convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
446.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2687
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 2567 is not initialized when it is used by options at mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c in line 462.

	Source	Destination
File	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c
Line	2575	491
Object	null	options

Code Snippet

File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c

Method static PyObject* _cbson_decode_all(PyObject* self, PyObject* args) {

```
....
2575.      PyObject* options_obj = NULL;
```

File Name mongodb@@mongo-python-driver-4.2.0-CVE-2024-21506-TP.c

Method int convert_codec_options(PyObject* options_obj, void* p) {

```
....
491.      Py_INCREF(options->options_obj);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=2688
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 598 is not initialized when it is used by registry at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 558.

	Source	Destination
File	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Line	599	583
Object	null	registry

Code Snippet

File Name mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c

Method int convert_codec_options(PyObject* self, PyObject* options_obj, codec_options_t* options) {

```
....
599.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c

Method int cbson_convert_type_registry(PyObject* registry_obj, type_registry_t* registry) {

```
....
583.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2689
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 2800 is not initialized when it is used by options at mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c in line 598.

	Source	Destination
File	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Line	2808	629
Object	null	options

Code Snippet

File Name mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c

Method	static PyObject* _cbson_decode_all(PyObject* self, PyObject* args) {

```
....
2808.       PyObject* options_obj = NULL;
```

File Name	mongodb@@mongo-python-driver-4.4.0-CVE-2024-21506-TP.c
Method	int convert_codec_options(PyObject* self, PyObject* options_obj, codec_options_t* options) {

```
....
629.       Py_INCREF(options->options_obj);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2690
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 680 is not initialized when it is used by registry at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 640.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Line	681	665
Object	null	registry

Code Snippet	
File Name	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Method	int convert_codec_options(PyObject* self, PyObject* options_obj, codec_options_t* options) {

```
....
681.       PyObject* type_registry_obj = NULL;
```

File Name	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Method	int cbson_convert_type_registry(PyObject* registry_obj, type_registry_t* registry, PyObject* _encoder_map_str, PyObject* _decoder_map_str, PyObject* _fallback_encoder_str) {

```
....
665.       Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2691
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 2920 is not initialized when it is used by options at mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c in line 680.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c
Line	2928	712
Object	null	options

Code Snippet

File Name mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c

Method static PyObject* _cbson_decode_all(PyObject* self, PyObject* args) {

```
....
2928.       PyObject* options_obj = NULL;
```

File Name mongodb@@mongo-python-driver-4.6.0-CVE-2024-21506-TP.c

Method int convert_codec_options(PyObject* self, PyObject* options_obj, codec_options_t* options) {

```
....
712.       Py_INCREF(options->options_obj);
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2692
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 680 is not initialized when it is used by registry at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 640.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Line	681	665
Object	null	registry

Code Snippet
File Name mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* self, PyObject* options_obj, codec_options_t* options) {

```
....
681.      PyObject* type_registry_obj = NULL;
```

File Name mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Method int cbson_convert_type_registry(PyObject* registry_obj, type_registry_t* registry, PyObject* _encoder_map_str, PyObject* _decoder_map_str, PyObject* _fallback_encoder_str) {

```
....
665.      Py_INCREF(registry->registry_obj);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2693
Status	New

The variable declared in null at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 2920 is not initialized when it is used by options at mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c in line 680.

	Source	Destination
File	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Line	2928	712
Object	null	options

Code Snippet
File Name mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Method static PyObject* _cbson_decode_all(PyObject* self, PyObject* args) {

```
....
2928.      PyObject* options_obj = NULL;
```

File Name mongodb@@mongo-python-driver-4.6.2-CVE-2024-21506-TP.c
Method int convert_codec_options(PyObject* self, PyObject* options_obj, codec_options_t* options) {

```
....
712.      Py_INCREF(options->options_obj);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2694
Status	New

The variable declared in 0 at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 12823 is not initialized when it is used by compressor at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 12823.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12832	12832
Object	0	compressor

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method flate_open_stream(FILE *out) /* I - Output file */

```
....
12832.    compressor.zalloc = (alloc_func)0;
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2695
Status	New

The variable declared in 0 at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 12823 is not initialized when it is used by compressor at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 12823.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12833	12833
Object	0	compressor

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c

Method	flate_open_stream(FILE *out) /* I - Output file */

```
....
12833.    compressor.zfree  = (free_func)0;
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2696
Status	New

The variable declared in 0 at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 12823 is not initialized when it is used by compressor at michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c in line 12823.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12834	12834
Object	0	compressor

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method	flate_open_stream(FILE *out) /* I - Output file */

```
....
12834.    compressor.opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2697
Status	New

The variable declared in 0 at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 12763 is not initialized when it is used by compressor at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 12763.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12772	12772
Object	0	compressor

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	flate_open_stream(FILE *out) /* I - Output file */

```
....
12772.    compressor.zalloc = (alloc_func)0;
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2698
Status	New

The variable declared in 0 at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 12763 is not initialized when it is used by compressor at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 12763.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12773	12773
Object	0	compressor

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	flate_open_stream(FILE *out) /* I - Output file */

```
....
12773.    compressor.zfree  = (free_func)0;
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2699
Status	New

The variable declared in 0 at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 12763 is not initialized when it is used by compressor at michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c in line 12763.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12774	12774
Object	0	compressor

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method flate_open_stream(FILE *out) /* I - Output file */

```
....
12774.    compressor.opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2700
Status New

The variable declared in 0 at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 12763 is not initialized when it is used by compressor at michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c in line 12763.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12772	12772
Object	0	compressor

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method flate_open_stream(FILE *out) /* I - Output file */

```
....
12772.    compressor.zalloc = (alloc_func)0;
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6182
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-	michaelrsweet@@htmldoc-v1.9.13-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	11341	11341
Object	HeadFootStyle	HeadFootStyle

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11341.    fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6183
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11346	11346
Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6184
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11284	11284
Object	HeadFootStyle	HeadFootStyle

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11284.    fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6185
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11289	11289
Object	style	style

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11289.      fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6186
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11284	11284
Object	HeadFootStyle	HeadFootStyle

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method	write_prolog(FILE *out, /* I - Output file */

```
....
11284.    fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6187
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11289	11289
Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11289.      fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6188
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11284	11284
Object	HeadFootStyle	HeadFootStyle

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11284.    fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6189
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11289	11289
Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11289.      fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6190
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11284	11284
Object	HeadFootStyle	HeadFootStyle

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11284.    fonts_used[HeadFootType][HeadFootStyle] = 1;
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6191
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11289	11289

Object	style	style

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11289.      fonts_used[r->data.text.typeface][r->data.text.style] = 1;
```

Unchecked Array Index\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6192
Status New

	Source	Destination
File	minetest@@minetest-5.2.0-CVE-2022-24300-TP.c	minetest@@minetest-5.2.0-CVE-2022-24300-TP.c
Line	73	73
Object	name	name

Code Snippet
File Name minetest@@minetest-5.2.0-CVE-2022-24300-TP.c
Method void ItemStackMetadata::deSerialize(std::istream &is)

```
....
73.                     m_stringvars[name] = var;
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6193
Status New

	Source	Destination
File	minetest@@minetest-5.3.0-CVE-2022-24300-TP.c	minetest@@minetest-5.3.0-CVE-2022-24300-TP.c
Line	73	73
Object	name	name

Code Snippet
File Name minetest@@minetest-5.3.0-CVE-2022-24300-TP.c
Method void ItemStackMetadata::deSerialize(std::istream &is)

```
....
73.                     m_stringvars[name] = var;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6194
Status	New

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	6151	6151
Object	maskOR_msb_offset	maskOR_msb_offset

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Method int mp_prime_random_ex(mp_int *a, int t, int size, int flags, ltm_prime_callback cb, void *dat)

```
....
6151.         tmp[maskOR_msb_offset]    |= maskOR_msb;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6195
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3042	3042
Object	_cbson_buffer_write_bytes_INDEX	_cbson_buffer_write_bytes_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3042.       _cbson_API[_cbson_buffer_write_bytes_INDEX] = (void *)
buffer_write_bytes;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6196
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3043	3043
Object	_cbson_write_dict_INDEX	_cbson_write_dict_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3043.       _cbson_API[_cbson_write_dict_INDEX] = (void *) write_dict;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6197
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3044	3044
Object	_cbson_write_pair_INDEX	_cbson_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3044.       _cbson_API[_cbson_write_pair_INDEX] = (void *) write_pair;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6198
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3045	3045
Object	_cbson_decode_and_write_pair_INDEX	_cbson_decode_and_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3045.       _cbson_API[_cbson_decode_and_write_pair_INDEX] = (void *)
decode_and_write_pair;
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6199
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3046	3046
Object	_cbson_convert_codec_options_INDEX	_cbson_convert_codec_options_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3046.       _cbson_API[_cbson_convert_codec_options_INDEX] = (void *)
convert_codec_options;
```

Unchecked Array Index\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6200
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c

Line	3047	3047
Object	_cbson_destroy_codec_options_INDEX	_cbson_destroy_codec_options_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3047.       _cbson_API[_cbson_destroy_codec_options_INDEX] = (void *)
destroy_codec_options;
```

Unchecked Array Index\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6201
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3048	3048
Object	_cbson_buffer_write_double_INDEX	_cbson_buffer_write_double_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3048.       _cbson_API[_cbson_buffer_write_double_INDEX] = (void *)
buffer_write_double;
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6202
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3049	3049
Object	_cbson_buffer_write_int32_INDEX	_cbson_buffer_write_int32_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3049.       _cbson_API[_cbson_buffer_write_int32_INDEX] = (void *)
buffer_write_int32;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6203
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3050	3050
Object	_cbson_buffer_write_int64_INDEX	_cbson_buffer_write_int64_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3050.       _cbson_API[_cbson_buffer_write_int64_INDEX] = (void *)
buffer_write_int64;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6204
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3051	3051
Object	_cbson_buffer_write_int32_at_position_INDEX	_cbson_buffer_write_int32_at_position_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3051.       _cbson_API[_cbson_buffer_write_int32_at_position_INDEX] =
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6205
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Line	3053	3053
Object	_cbson_downcast_and_check_INDEX	_cbson_downcast_and_check_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.0-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3053.       _cbson_API[_cbson_downcast_and_check_INDEX] = (void *)
_downcast_and_check;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6206
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3043	3043
Object	_cbson_buffer_write_bytes_INDEX	_cbson_buffer_write_bytes_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3043.       _cbson_API[_cbson_buffer_write_bytes_INDEX] = (void *)
buffer_write_bytes;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6207
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3044	3044
Object	_cbson_write_dict_INDEX	_cbson_write_dict_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3044.       _cbson_API[_cbson_write_dict_INDEX] = (void *) write_dict;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6208
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3045	3045
Object	_cbson_write_pair_INDEX	_cbson_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3045.       _cbson_API[_cbson_write_pair_INDEX] = (void *) write_pair;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6209
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3046	3046
Object	_cbson_decode_and_write_pair_INDEX	_cbson_decode_and_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3046.       _cbson_API[_cbson_decode_and_write_pair_INDEX] = (void *)
decode_and_write_pair;
```

Unchecked Array Index\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6210
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3047	3047
Object	_cbson_convert_codec_options_INDEX	_cbson_convert_codec_options_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3047.       _cbson_API[_cbson_convert_codec_options_INDEX] = (void *)
convert_codec_options;
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6211
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c

Line	3048	3048
Object	_cbson_destroy_codec_options_INDEX	_cbson_destroy_codec_options_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3048.       _cbson_API[_cbson_destroy_codec_options_INDEX] = (void *)
destroy_codec_options;
```

Unchecked Array Index\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6212
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3049	3049
Object	_cbson_buffer_write_double_INDEX	_cbson_buffer_write_double_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3049.       _cbson_API[_cbson_buffer_write_double_INDEX] = (void *)
buffer_write_double;
```

Unchecked Array Index\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6213
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3050	3050
Object	_cbson_buffer_write_int32_INDEX	_cbson_buffer_write_int32_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3050.       _cbson_API[_cbson_buffer_write_int32_INDEX] = (void *)
buffer_write_int32;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6214
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3051	3051
Object	_cbson_buffer_write_int64_INDEX	_cbson_buffer_write_int64_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3051.       _cbson_API[_cbson_buffer_write_int64_INDEX] = (void *)
buffer_write_int64;
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6215
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3052	3052
Object	_cbson_buffer_write_int32_at_position_INDEX	_cbson_buffer_write_int32_at_position_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3052.       _cbson_API[_cbson_buffer_write_int32_at_position_INDEX] =
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6216
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Line	3054	3054
Object	_cbson_downcast_and_check_INDEX	_cbson_downcast_and_check_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3054.       _cbson_API[_cbson_downcast_and_check_INDEX] = (void *)
_downcast_and_check;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6217
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3043	3043
Object	_cbson_buffer_write_bytes_INDEX	_cbson_buffer_write_bytes_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3043.       _cbson_API[_cbson_buffer_write_bytes_INDEX] = (void *)
buffer_write_bytes;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6218
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3044	3044
Object	_cbson_write_dict_INDEX	_cbson_write_dict_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3044.       _cbson_API[_cbson_write_dict_INDEX] = (void *) write_dict;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6219
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3045	3045
Object	_cbson_write_pair_INDEX	_cbson_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3045.       _cbson_API[_cbson_write_pair_INDEX] = (void *) write_pair;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6220
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3046	3046
Object	_cbson_decode_and_write_pair_INDEX	_cbson_decode_and_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3046.       _cbson_API[_cbson_decode_and_write_pair_INDEX] = (void *)
decode_and_write_pair;
```

Unchecked Array Index\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6221
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3047	3047
Object	_cbson_convert_codec_options_INDEX	_cbson_convert_codec_options_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3047.       _cbson_API[_cbson_convert_codec_options_INDEX] = (void *)
convert_codec_options;
```

Unchecked Array Index\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6222
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c

Line	3048	3048
Object	_cbson_destroy_codec_options_INDEX	_cbson_destroy_codec_options_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3048.       _cbson_API[_cbson_destroy_codec_options_INDEX] = (void *)
destroy_codec_options;
```

Unchecked Array Index\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6223
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3049	3049
Object	_cbson_buffer_write_double_INDEX	_cbson_buffer_write_double_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3049.       _cbson_API[_cbson_buffer_write_double_INDEX] = (void *)
buffer_write_double;
```

Unchecked Array Index\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6224
Status New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3050	3050
Object	_cbson_buffer_write_int32_INDEX	_cbson_buffer_write_int32_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3050.       _cbson_API[_cbson_buffer_write_int32_INDEX] = (void *)
buffer_write_int32;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6225
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3051	3051
Object	_cbson_buffer_write_int64_INDEX	_cbson_buffer_write_int64_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3051.       _cbson_API[_cbson_buffer_write_int64_INDEX] = (void *)
buffer_write_int64;
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6226
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3052	3052
Object	_cbson_buffer_write_int32_at_position_INDEX	_cbson_buffer_write_int32_at_position_INDEX

Code Snippet

File Name	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method	PyInit__cbson(void)

```
....
3052.       _cbson_API[_cbson_buffer_write_int32_at_position_INDEX] =
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6227
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Line	3054	3054
Object	_cbson_downcast_and_check_INDEX	_cbson_downcast_and_check_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.11.4-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3054.       _cbson_API[_cbson_downcast_and_check_INDEX] = (void *)
_downcast_and_check;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6228
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Line	3043	3043
Object	_cbson_buffer_write_bytes_INDEX	_cbson_buffer_write_bytes_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3043.       _cbson_API[_cbson_buffer_write_bytes_INDEX] = (void *)
buffer_write_bytes;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6229
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Line	3044	3044
Object	_cbson_write_dict_INDEX	_cbson_write_dict_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3044.       _cbson_API[_cbson_write_dict_INDEX] = (void *) write_dict;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6230
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Line	3045	3045
Object	_cbson_write_pair_INDEX	_cbson_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3045.       _cbson_API[_cbson_write_pair_INDEX] = (void *) write_pair;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6231
Status	New

	Source	Destination
File	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c	mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Line	3046	3046
Object	_cbson_decode_and_write_pair_INDEX	_cbson_decode_and_write_pair_INDEX

Code Snippet
File Name mongodb@@mongo-python-driver-3.12.1-CVE-2024-21506-TP.c
Method PyInit__cbson(void)

```
....
3046.       _cbson_API[_cbson_decode_and_write_pair_INDEX] = (void *)
decode_and_write_pair;
```

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=1020042&projectid=20035&pathid=3127
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	787	787
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
787.    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=1020042&projectid=20035&pathid=3128
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3129
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3130
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	758	758

Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3131
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3132
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3133
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3134
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3135
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Line	758	758
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3136
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	912	912
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
912.    strlcat(newfilename, slash, sizeof(newfilename));
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3137
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	912	912
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
912.    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=1020042&projectid=20035&pathid=3138
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	912	912
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.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=1020042&projectid=20035&pathid=3139
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	916	916

Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
916.    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=1020042&projectid=20035&pathid=3140
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	904	904
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
904.    strlcat(newfilename, slash, sizeof(newfilename));
```

Sizeof Pointer Argument\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3141
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	776	776
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
776.    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=1020042&projectid=20035&pathid=3142
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	650	650
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
650.      strlcpy(basename, s, sizeof(basename));
```

Sizeof Pointer Argument\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3143
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3144
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3145
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3146
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3147
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	638	638
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3148
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	747	747

Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3149
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3150
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3151
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Line	747	747
Object	header	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3152
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	643	643
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 27:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3153
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	701	701
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3154
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	643	643
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-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=1020042&projectid=20035&pathid=3155
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	701	701
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-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=1020042&projectid=20035&pathid=3156
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	643	643
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-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 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3157
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	701	701

Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-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 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3158
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	705	705
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
705.      filename[sizeof(filename) - 1] = '\0';
```

Sizeof Pointer Argument\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3159
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	693	693
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3160
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	648	648
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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=1020042&projectid=20035&pathid=3161
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	908	908
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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=1020042&projectid=20035&pathid=3162
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	648	648
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-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 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3163
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	908	908
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
908.        strlcat(newfilename, "../", sizeof(newfilename));
```

Sizeof Pointer Argument\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3164
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	648	648
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-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 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3165
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	908	908
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
908.        strlcat(newfilename, "../", sizeof(newfilename));
```

Sizeof Pointer Argument\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3166
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	654	654

Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_find(const char *path, /* I - Path "dir;dir;dir" */

```
....
654.          *sptr && temp < (basename + sizeof(basename) - 1);)
```

Sizeof Pointer Argument\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3167
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	912	912
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
912.          strlcat(newfilename, "../", sizeof(newfilename));
```

Sizeof Pointer Argument\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3168
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	642	642
Object	basename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3169
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	900	900
Object	newfilename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Method file_localize(const char *filename, /* I - Filename */

```
....
900.          strlcat(newfilename, "../", sizeof(newfilename));
```

Sizeof Pointer Argument\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3170
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	980	980
Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 45:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3171
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.17-CVE-2021-23180-FP.c
Line	980	980
Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.17-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 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3172
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.18-CVE-2021-23180-FP.c
Line	980	980
Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.18-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 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3173
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Line	982	982
Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23180-TP.c
Method file_proxy(const char *url) /* I - URL of proxy server */

```
....
982.        strlcpy(proxy_host, hostname, sizeof(proxy_host));
```

Sizeof Pointer Argument\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3174
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23180-TP.c
Line	970	970
Object	proxy_host	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3175
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	711	711

Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.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 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3176
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.c
Line	725	711
Object	filename	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2021-23180-FP.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))
```

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=1020042&projectid=20035&pathid=2804

Status	New

The size of the buffer used by image_load_gif in height, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1282	1373
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1282.    fread(buf, 13, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2805
Status	New

The size of the buffer used by image_load_gif in height, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1322	1373
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1322.            fread(buf, 9, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2806
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1282	1373
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1282.    fread(buf, 13, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2807
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1322	1373
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1322.            fread(buf, 9, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2808
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1282	1373
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1282.    fread(buf, 13, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2809
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

Line	1322	1373
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1322.            fread(buf, 9, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2810
Status	New

The size of the buffer used by image_load_gif in long, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1282	1373
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1282.    fread(buf, 13, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2811
Status	New

The size of the buffer used by image_load_gif in long, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1322	1373
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1322.            fread(buf, 9, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2812
Status New

The size of the buffer used by image_load_gif in width, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1282	1373
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1282.    fread(buf, 13, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2813
Status	New

The size of the buffer used by image_load_gif in width, at line 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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 1267 of michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	1322	1373
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load_gif(image_t *img, /* I - Image pointer */

```
....
1322.            fread(buf, 9, 1, fp);
....
1373.            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=1020042&projectid=20035&pathid=2814
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2815
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2816
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2817
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2818
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2819
Status New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 17:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2820
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2821
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2822
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2823
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c

Line	1279	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2824
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2825
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2826
Status New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2827
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2828
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2829
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2830
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c

Line	1242	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2831
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2832
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2833
Status New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	1279	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2834
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2835
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2836
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2837
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c

Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2838
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2839
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2840
Status New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 38:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2841
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2842
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2843
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	1279	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2844
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c

Line	1242	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2845
Status	New

The size of the buffer used by image_load_gif in height, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	height

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2846
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2847
Status New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2848
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2849
Status	New

The size of the buffer used by image_load_gif in BinaryExpr, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	BinaryExpr

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2850
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2851
Status	New

The size of the buffer used by image_load_gif in long, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c

Line	1279	1326
Object	buf	long

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2852
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1242	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2853
Status	New

The size of the buffer used by image_load_gif in width, at line 1227 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c, to overwrite the target buffer.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	1279	1326
Object	buf	width

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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));
```

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=1020042&projectid=20035&pathid=5844
Status	New

The pspdf_export method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	584	584
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5845
Status	New

The pdf_write_document method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2392	2392
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pdf_write_document(uchar *author, // I - Author of document

```
....
2392.       out = fopen(stdout_filename, "rb");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5846
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9812	9812
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9812.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5847
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9818	9818
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9818.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5848
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	9821	9821
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9821.       return (fopen(OutputPath, "wb+"));
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5849
Status	New

The write_prolog method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11674	11674
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11674.        if ((prolog = fopen(temp, "rb")) != NULL)
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5850
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12459	12459
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12459.    if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5851
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12581	12581
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12581.      if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5852
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	580	580
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
580.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5853
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	587	587
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
587.    if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5854
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-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-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	768	768
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c

Method	image_load(const char *filename,/* I - Name of image file */

```
....
768.    if ((fp = fopen(realname, "rb")) == NULL)
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5855
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	551	551
Object	fopen	fopen

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method	image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5856
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	558	558
Object	fopen	fopen

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Method	image_copy(const char *src, /* I - Source file */

```
....
558.    if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5857
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	739	739
Object	fopen	fopen

Code Snippet

File Name	michaelrsweet@@htmldoc-v1.9.8-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5858
Status	New

The pspdf_export method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	584	584
Object	fopen	fopen

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5859
Status	New

The pdf_write_document method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2390	2390
Object	fopen	fopen

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	pdf_write_document(uchar *author, // I - Author of document

```
....
2390.       out = fopen(stdout_filename, "rb");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5860
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	9755	9755
Object	fopen	fopen

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	open_file(void)

```
....
9755.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5861
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	9761	9761
Object	fopen	fopen

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method	open_file(void)

```
....
9761.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5862
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	9764	9764

Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9764.       return (fopen(OutputPath, "wb+"));
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5863
Status	New

The write_prolog method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11617	11617
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out,   /* I - Output file */

```
....
11617.        if ((prolog = fopen(temp, "rb")) != NULL)
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5864
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c

Line	12399	12399
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12399.    if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5865
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12521	12521
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12521.      if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5866
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-	michaelrsweet@@htmldoc-v1.9.8-CVE-

	2022-0137-TP.c	2022-0137-TP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5867
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	558	558
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.    if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5868
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	739	739
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5869
Status New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5870
Status New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	558	558
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.    if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5871
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	739	739
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5872
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5873
Status	New

The image_copy method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	558	558
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.    if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5874
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	739	739
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5875
Status	New

The pspdf_export method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	584	584
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5876
Status	New

The pdf_write_document method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	2390	2390
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pdf_write_document(uchar *author, // I - Author of document

```
....
2390.       out = fopen(stdout_filename, "rb");
```

TOCTOU\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5877
Status New

The open_file method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	9755	9755
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9755.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5878
Status New

The open_file method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	9761	9761
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9761.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5879
Status	New

The open_file method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	9764	9764
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method open_file(void)

```
....
9764.       return (fopen(OutputPath, "wb+"));
```

TOCTOU\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5880
Status	New

The write_prolog method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11617	11617
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11617.        if ((prolog = fopen(temp, "rb")) != NULL)
```

TOCTOU\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5881
Status New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12399	12399
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12399.    if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5882
Status New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12521	12521
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12521.      if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5883
Status New

The image_copy method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
551.    if ((in = fopen(realsrc, "rb")) == NULL)
```

TOCTOU\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5884
Status New

The image_copy method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	558	558
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Method image_copy(const char *src, /* I - Source file */

```
....
558.    if ((out = fopen(dest, "wb")) == NULL)
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5885
Status	New

The image_load method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	739	739
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5886
Status	New

The pspdf_export method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	584	584
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5887
Status New

The pdf_write_document method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	2390	2390
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pdf_write_document(uchar *author, // I - Author of document

```
....
2390.       out = fopen(stdout_filename, "rb");
```

TOCTOU\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5888
Status New

The open_file method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	9755	9755
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9755.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5889
Status New

The open_file method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	9761	9761
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9761.       return (fopen(filename, "wb+"));
```

TOCTOU\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5890
Status New

The open_file method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	9764	9764
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method open_file(void)

```
....
9764.       return (fopen(OutputPath, "wb+"));
```

TOCTOU\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5891
Status New

The write_prolog method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11617	11617
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11617.        if ((prolog = fopen(temp, "rb")) != NULL)
```

TOCTOU\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5892
Status New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12399	12399
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12399.    if ((fp = fopen(filename, "r")) == NULL)
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5893
Status	New

The write_type1 method in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12521	12521
Object	fopen	fopen

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12521.      if ((fp = fopen(filename, "r")) == 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=1020042&projectid=20035&pathid=5743
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	223	223
Object	chmod	chmod

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5744
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	223	223
Object	chmod	chmod

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5745
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	221	221
Object	chmod	chmod

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpAddrListen(http_addr_t *addr, /* I - Address to bind to */

```
....
221.      chmod(addr->un.sun_path, 0140777);
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5746
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	221	221
Object	chmod	chmod

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Method httpAddrListen(http_addr_t *addr, /* I - Address to bind to */

```
....
221.      chmod(addr->un.sun_path, 0140777);
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5747
Status New

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	967	967

Object	chmod	chmod

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method sink(int argc, char **argv)

```
....
967.                                    (void) chmod(np, mode);
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5748
Status New

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	984	984
Object	chmod	chmod

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method sink(int argc, char **argv)

```
....
984.                                (void) chmod(vect[0], mode);
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5749
Status New

	Source	Destination
File	MisterTea@@EternalTerminal-et-v6.0.12-CVE-2022-24950-TP.c	MisterTea@@EternalTerminal-et-v6.0.12-CVE-2022-24950-TP.c
Line	13	13
Object	chmod	chmod

Code Snippet
File Name MisterTea@@EternalTerminal-et-v6.0.12-CVE-2022-24950-TP.c
Method UserTerminalRouter::UserTerminalRouter(

```
....
13.    FATAL_FAIL(::chmod(_routerEndpoint.name().c_str(),
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5750
Status	New

	Source	Destination
File	MisterTea@@EternalTerminal-et-v6.0.8-CVE-2022-24950-TP.c	MisterTea@@EternalTerminal-et-v6.0.8-CVE-2022-24950-TP.c
Line	13	13
Object	chmod	chmod

Code Snippet
File Name MisterTea@@EternalTerminal-et-v6.0.8-CVE-2022-24950-TP.c
Method UserTerminalRouter::UserTerminalRouter(

```
....
13.    FATAL_FAIL(::chmod(_routerEndpoint.name().c_str(),
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5751
Status	New

	Source	Destination
File	MisterTea@@EternalTerminal-et-v6.1.0-CVE-2022-24950-FP.c	MisterTea@@EternalTerminal-et-v6.1.0-CVE-2022-24950-FP.c
Line	13	13
Object	chmod	chmod

Code Snippet
File Name MisterTea@@EternalTerminal-et-v6.1.0-CVE-2022-24950-FP.c
Method UserTerminalRouter::UserTerminalRouter(

```
....
13.    FATAL_FAIL(::chmod(_routerEndpoint.name().c_str(),
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5752
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	584	584
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5753
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2392	2392
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5754
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11674	11674
Object	prolog	prolog

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11674.        if ((prolog = fopen(temp, "rb")) != NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5755
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12459	12459
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5756
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	12581	12581

Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-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 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5757
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	580	580
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
580.    if ((in = fopen(realsrc, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5758
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	587	587
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_copy(const char *src, /* I - Source file */

```
....
587.    if ((out = fopen(dest, "wb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5759
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	768	768
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
768.    if ((fp = fopen(realname, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5760
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	551	551
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5761
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5762
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5763
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	584	584
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5764
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2390	2390
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5765
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11617	11617

Object	prolog	prolog

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11617.        if ((prolog = fopen(temp, "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=1020042&projectid=20035&pathid=5766
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12399	12399
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12399.    if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5767
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	12521	12521
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12521.      if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5768
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	551	551
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5769
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5770
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5771
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	551	551
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5772
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5773
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5774
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	551	551

Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5775
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5776
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5777
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	584	584
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5778
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	2390	2390
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5779
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11617	11617
Object	prolog	prolog

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11617.        if ((prolog = fopen(temp, "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=1020042&projectid=20035&pathid=5780
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12399	12399
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12399.    if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5781
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	12521	12521
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12521.      if ((fp = fopen(filename, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5782
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	551	551
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5783
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	558	558

Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5784
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	739	739
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5785
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	584	584
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5786
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	2390	2390
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5787
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11617	11617
Object	prolog	prolog

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11617.        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=1020042&projectid=20035&pathid=5788
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12399	12399
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12399.    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=1020042&projectid=20035&pathid=5789
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	12521	12521
Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_type1(FILE *out, /* I - File to write to */

```
....
12521.      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=1020042&projectid=20035&pathid=5790
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	551	551
Object	in	in

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5791
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	558	558
Object	out	out

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5792
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	739	739

Object	fp	fp

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
739.    if ((fp = fopen(realname, "rb")) == NULL)
```

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=1020042&projectid=20035&pathid=6130
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	2886	2886
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6131
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6540	6540
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.13-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 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6132
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6542	6542
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.13-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 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6133
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	6552	6552
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.13-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 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6134
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	809	809
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
809.        temp = (image_t **)malloc(sizeof(image_t *) * alloc_images);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6135
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Line	811	811
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-CVE-2022-0137-FP.c
Method image_load(const char *filename,/* I - Name of image file */

```
....
811.        temp = (image_t **)realloc(images, sizeof(image_t *) *
alloc_images);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6136
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6137
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23191-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6138

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	2884	2884
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6139
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	6497	6497
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6497.          cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6140
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-	michaelrsweet@@htmldoc-v1.9.8-CVE-

	2021-23206-TP.c	2021-23206-TP.c
Line	6499	6499
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6499.          cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6141
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	6509	6509
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6509.        if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6142
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6143
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0137-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6144
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.8-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 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6145
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-0534-FP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6146
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6147
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-27114-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6148
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	2884	2884
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6149

Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	6497	6497
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6497.         cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6150
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	6499	6499
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6499.         cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6151
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-	michaelrsweet@@htmldoc-v1.9.8-CVE-

	2022-28085-TP.c	2022-28085-TP.c
Line	6509	6509
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6509.         if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6152
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6153
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23191-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6154
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	2884	2884
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6155
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	6497	6497
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6497.          cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6156
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	6499	6499
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6499.          cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6157
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	6509	6509
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6509.          if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6158
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6159
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0137-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=6160
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6161
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-0534-FP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6162
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-	michaelrsweet@@htmldoc-v1.9.9-CVE-

	2022-27114-TP.c	2022-27114-TP.c
Line	780	780
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6163
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-27114-TP.c
Line	782	782
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-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 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6164
Status New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	2884	2884
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.9-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 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6165
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	6497	6497
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6497.          cells = (tree_t ***)malloc(sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6166
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	6499	6499
Object	sizeof	sizeof

Code Snippet	
File Name	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method	parse_table(tree_t *t, // I - Tree to parse

```
....
6499.         cells = (tree_t ***)realloc(cells, sizeof(tree_t **) *
(size_t)alloc_rows);
```

Use of Sizeof On a Pointer Type\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6167
Status	New

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	6509	6509
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method parse_table(tree_t *t, // I - Tree to parse

```
....
6509.         if ((cells[table.num_rows] = (tree_t
**)calloc(sizeof(tree_t *), MAX_COLUMNS)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6168
Status	New

	Source	Destination
File	michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c	michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c
Line	147	147
Object	sizeof	sizeof

Code Snippet
File Name michaelrsweet@@pdfio-v1.0.0-CVE-2023-24808-TP.c
Method pdfioDictCreate(pdfio_file_t *pdf) // I - PDF file

```
....
147.      pdfio_dict_t **temp = (pdfio_dict_t **)realloc(pdf->dicts,
(pdf->alloc_dicts + 16) * sizeof(pdfio_dict_t *));
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6169
Status	New

	Source	Destination
File	minetest@@minetest-5.5.0-CVE-2022-35978-TP.c	minetest@@minetest-5.5.0-CVE-2022-35978-TP.c
Line	86	86
Object	sizeof	sizeof

Code Snippet
File Name minetest@@minetest-5.5.0-CVE-2022-35978-TP.c
Method void LuaSettings::create(lua_State *L, Settings *settings,

```
....
86.    *(void **)(lua_newuserdata(L, sizeof(void *))) = o;
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6170
Status	New

	Source	Destination
File	minetest@@minetest-5.5.0-CVE-2022-35978-TP.c	minetest@@minetest-5.5.0-CVE-2022-35978-TP.c
Line	353	353
Object	sizeof	sizeof

Code Snippet
File Name minetest@@minetest-5.5.0-CVE-2022-35978-TP.c
Method int LuaSettings::create_object(lua_State* L)

```
....
353.        *(void **)(lua_newuserdata(L, sizeof(void *))) = o;
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6171

Status	New

	Source	Destination
File	minetest@@minetest-5.5.1-CVE-2022-35978-TP.c	minetest@@minetest-5.5.1-CVE-2022-35978-TP.c
Line	86	86
Object	sizeof	sizeof

Code Snippet
File Name minetest@@minetest-5.5.1-CVE-2022-35978-TP.c
Method void LuaSettings::create(lua_State *L, Settings *settings,

```
....
86.    *(void **)(lua_newuserdata(L, sizeof(void *))) = o;
```

Use of Sizeof On a Pointer Type\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6172
Status	New

	Source	Destination
File	minetest@@minetest-5.5.1-CVE-2022-35978-TP.c	minetest@@minetest-5.5.1-CVE-2022-35978-TP.c
Line	353	353
Object	sizeof	sizeof

Code Snippet
File Name minetest@@minetest-5.5.1-CVE-2022-35978-TP.c
Method int LuaSettings::create_object(lua_State* L)

```
....
353.        *(void **)(lua_newuserdata(L, sizeof(void *))) = o;
```

Use of Sizeof On a Pointer Type\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6173
Status	New

	Source	Destination
File	mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c	mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c

Line	2968	2968
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c
Method scope_add_irep(codegen_scope *s, mrb_irep *irep)

```
....
2968.       s->irep->reps = (mrb_irep**)codegen_realloc(s, s->irep->reps,
sizeof(mrb_irep*)*s->rcapa);
```

Use of Sizeof On a Pointer Type\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6174
Status	New

	Source	Destination
File	mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c	mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c
Line	2998	2998
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c
Method scope_new(mrb_state *mrb, codegen_scope *prev, node *lv)

```
....
2998.     p->irep->reps = (mrb_irep**)mrb_malloc(mrb,
sizeof(mrb_irep*)*p->rcapa);
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6175
Status	New

	Source	Destination
File	mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c	mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c
Line	3071	3071
Object	sizeof	sizeof

Code Snippet

File Name	mruby@@mruby-2.1.1-rc-CVE-2022-0481-FP.c
Method	scope_finish(codegen_scope *s)

```
....
3071.    irep->reps = (mrb_irep**)codegen_realloc(s, irep->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6176
Status	New

	Source	Destination
File	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c
Line	2996	2996
Object	sizeof	sizeof

Code Snippet

File Name	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c
Method	scope_add_irep(codegen_scope *s, mrb_irep *irep)

```
....
2996.      s->irep->reps = (mrb_irep**)codegen_realloc(s, s->irep->reps,
sizeof(mrb_irep*)*s->rcapa);
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6177
Status	New

	Source	Destination
File	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c
Line	3026	3026
Object	sizeof	sizeof

Code Snippet

File Name	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c
Method	scope_new(mrb_state *mrb, codegen_scope *prev, node *lv)

```
....
3026.    p->irep->reps = (mrb_irep**)mrb_malloc(mrb,
sizeof(mrb_irep*)*p->rcapa);
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6178
Status	New

	Source	Destination
File	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c	mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c
Line	3099	3099
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-2.1.2-rc2-CVE-2022-0481-FP.c
Method scope_finish(codegen_scope *s)

```
....
3099.    irep->reps = (mrb_irep**)codegen_realloc(s, irep->reps,
sizeof(mrb_irep*)*irep->rlen);
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=6179
Status	New

	Source	Destination
File	mruby@@mruby-3.0.0-rc-CVE-2022-0481-FP.c	mruby@@mruby-3.0.0-rc-CVE-2022-0481-FP.c
Line	3042	3042
Object	sizeof	sizeof

Code Snippet
File Name mruby@@mruby-3.0.0-rc-CVE-2022-0481-FP.c
Method scope_add_irep(codegen_scope *s)

```
....
3042.        prev->reps = (mrb_irep**)codegen_realloc(s, prev->reps,
sizeof(mrb_irep*)*prev->rcapa);
```

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=1020042&projectid=20035&pathid=5811
Status	New

The system data read by myread in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 50 is potentially exposed by myread found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 50.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	62	62
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
62.                     perror(prefix);
```

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=1020042&projectid=20035&pathid=5812
Status	New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	111	111

Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
111.                    perror(filename);
```

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=1020042&projectid=20035&pathid=5813
Status New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	133	133
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
133.              perror("malloc");
```

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=1020042&projectid=20035&pathid=5814
Status New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c

Line	140	140
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
140.              perror("lseek");
```

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=1020042&projectid=20035&pathid=5815
Status	New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	153	153
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
153.              perror(filename);
```

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=1020042&projectid=20035&pathid=5816
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-	mirror@@dmidecode-dmidecode-3-3-

	CVE-2023-30630-TP.c	CVE-2023-30630-TP.c
Line	186	186
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
186.                perror(devmem);
```

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=1020042&projectid=20035&pathid=5817
Status New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	192	192
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
192.                perror("malloc");
```

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=1020042&projectid=20035&pathid=5818
Status New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174.

	Source	Destination

File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	200	200
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
200.                perror("stat");
```

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=1020042&projectid=20035&pathid=5819
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	234	234
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
234.                perror("munmap");
```

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=1020042&projectid=20035&pathid=5820
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	244	244
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
244.                perror("lseek");
```

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=1020042&projectid=20035&pathid=5821
Status New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	257	257
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
257.                perror(devmem);
```

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=1020042&projectid=20035&pathid=5822
Status New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	270	270
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
270.                perror("fopen");
```

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=1020042&projectid=20035&pathid=5823
Status	New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	277	277
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
277.                perror("fseek");
```

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=1020042&projectid=20035&pathid=5824
Status	New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	284	284
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
284.                perror("fwrite");
```

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=1020042&projectid=20035&pathid=5825
Status New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	291	291
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
291.                perror("fclose");
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=5826
Status	New

The system data read by myread in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 50 is potentially exposed by myread found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 50.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	62	62
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
62.                     perror(prefix);
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5827
Status	New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	111	111
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
111.                    perror(filename);
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5828
Status	New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	133	133
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
133.              perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5829
Status	New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	140	140
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
140.              perror("lseek");
```

Exposure of System Data to Unauthorized Control Sphere\Path 20:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5830
Status	New

The system data read by *read_file in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98 is potentially exposed by *read_file found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 98.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	153	153
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *read_file(off_t base, size_t *max_len, const char *filename)

```
....
153.              perror(filename);
```

Exposure of System Data to Unauthorized Control Sphere\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5831
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	186	186
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
186.              perror(devmem);
```

Exposure of System Data to Unauthorized Control Sphere\Path 22:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5832
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	192	192
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
192.                perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5833
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	200	200
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
200.                perror("stat");
```

Exposure of System Data to Unauthorized Control Sphere\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5834
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	234	234
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
234.                perror("munmap");
```

Exposure of System Data to Unauthorized Control Sphere\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5835
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	244	244
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
244.                perror("lseek");
```

Exposure of System Data to Unauthorized Control Sphere\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5836
Status	New

The system data read by *mem_chunk in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174 is potentially exposed by *mem_chunk found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 174.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	257	257
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method void *mem_chunk(off_t base, size_t len, const char *devmem)

```
....
257.                perror(devmem);
```

Exposure of System Data to Unauthorized Control Sphere\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5837
Status	New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	270	270
Object	perror	perror

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
270.                perror("fopen");
```

Exposure of System Data to Unauthorized Control Sphere\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5838
Status	New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	277	277
Object	perror	perror

Code Snippet

File Name mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c

Method int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
277.                perror("fseek");
```

Exposure of System Data to Unauthorized Control Sphere\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5839
Status	New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	284	284
Object	perror	perror

Code Snippet

File Name	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method	int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
284.                perror("fwrite");
```

Exposure of System Data to Unauthorized Control Sphere\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5840
Status	New

The system data read by write_dump in the file mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262 is potentially exposed by write_dump found in mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c at line 262.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	291	291
Object	perror	perror

Code Snippet

File Name	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method	int write_dump(size_t base, size_t len, const void *data, const char *dumpfile, int add)

```
....
291.                perror("fclose");
```

Exposure of System Data to Unauthorized Control Sphere\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5841
Status	New

The system data read by do_local_cmd in the file mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c at line 118 is potentially exposed by do_local_cmd found in mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c at line 118.

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	143	143

Object	perror	perror

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method do_local_cmd(arglist *a)

```
....
143.              perror(a->list[0]);
```

Exposure of System Data to Unauthorized Control Sphere\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5842
Status	New

The system data read by do_cmd in the file mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c at line 175 is potentially exposed by do_cmd found in mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c at line 175.

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	236	236
Object	perror	perror

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Method do_cmd(char *host, char *remuser, char *cmd, int *fdin, int *fdout, int argc)

```
....
236.              perror(ssh_program);
```

Exposure of System Data to Unauthorized Control Sphere\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5843
Status	New

The system data read by LogHandler::createLogFile in the file MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c at line 84 is potentially exposed by LogHandler::createLogFile found in MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c at line 84.

	Source	Destination
File	MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c	MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c

Line	88	89
Object	fse	"stdout"

Code Snippet
File Name MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c
Method string LogHandler::createLogFile(const string &path, const string &filename) {

```
....
88.     } catch (const fs::filesystem_error &fse) {
89.       CLOG(ERROR, "stdout") << "Cannot create logfile directory: " <<
fse.what()
```

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=1020042&projectid=20035&pathid=2553
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1362.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2554
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1377.    for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2555
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1321	1321
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1321.            i <= chapter_ends[c];
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20

	035&pathid=2556
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1362.    for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2557
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1377.    for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2558

Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	1321	1321
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1321.           i <= chapter_ends[c];
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2559
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1362.     for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2560
Status	New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1377.    for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2561
Status New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	1321	1321
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1321.            i <= chapter_ends[c];
```

Potential Off by One Error in Loops\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2562
Status New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1362.    for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2563
Status New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method pspdf_prepare_outpages()

```
....
1377.    for (c = 0; c <= TocDocCount; c ++)
```

Potential Off by One Error in Loops\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2564
Status New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	1321	1321
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1321.           i <= chapter_ends[c];
```

Potential Off by One Error in Loops\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2565
Status New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	1362	1362
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1362.     for (c = 0; c <= TocDocCount; 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=1020042&projectid=20035&pathid=2566
Status New

The buffer allocated by <= in michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	1377	1377
Object	<=	<=

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method pspdf_prepare_outpages()

```
....
1377.    for (c = 0; c <= TocDocCount; c ++)
```

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=1020042&projectid=20035&pathid=5927
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11759	11759
Object	rand	rand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5928
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11702	11702
Object	rand	rand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11702.          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=1020042&projectid=20035&pathid=5929
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11702	11702
Object	rand	rand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11702.          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=1020042&projectid=20035&pathid=5930
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11702	11702
Object	rand	rand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11702.          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=1020042&projectid=20035&pathid=5931
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11702	11702
Object	rand	rand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11702.          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=1020042&projectid=20035&pathid=5932
Status	New

Method mp_rand at line 6324 of mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-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	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	6336	6336
Object	rand	rand

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Method mp_rand (mp_int * a, int digits)

```
....
6336.       d = ((mp_digit) abs (rand ())) & MP_MASK;
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5933
Status	New

Method mp_rand at line 6324 of mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-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	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c	mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Line	6348	6348
Object	rand	rand

Code Snippet
File Name mkj@@dropbear-maemo-0.52-2-CVE-2023-36328-TP.c
Method mp_rand (mp_int * a, int digits)

```
....
6348.       if ((res = mp_add_d (a, ((mp_digit) abs (rand ())), a)) !=
MP_OKAY) {
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5934
Status	New

Method write_prolog at line 11300 of michaelrsweet@@htmldoc-v1.9.13-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-v1.9.13-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Line	11756	11756
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11756.      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=1020042&projectid=20035&pathid=5935
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Line	11699	11699
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11699.      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=1020042&projectid=20035&pathid=5936
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.8-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-v1.9.8-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Line	11699	11699
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11699.      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=1020042&projectid=20035&pathid=5937
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2021-23206-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Line	11699	11699
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2021-23206-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11699.      srand(time(NULL));
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=5938
Status	New

Method write_prolog at line 11243 of michaelrsweet@@htmldoc-v1.9.9-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-v1.9.9-CVE-2022-28085-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Line	11699	11699
Object	srand	srand

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2022-28085-TP.c
Method write_prolog(FILE *out, /* I - Output file */

```
....
11699.      srand(time(NULL));
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read 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 read\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2894
Status	New

The size of the buffer used by myread in BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that myread passes to BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c, to overwrite the target buffer.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	57	57
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method	static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
57.          r = read(fd, buf + r2, count - r2);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2895
Status	New

The size of the buffer used by myread in BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that myread passes to BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c, to overwrite the target buffer.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	57	57
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method	static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
57.          r = read(fd, buf + r2, count - r2);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2896
Status	New

The size of the buffer used by myread in count, at line 50 of mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that myread passes to BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c, to overwrite the target buffer.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	57	57
Object	BinaryExpr	count

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
57.          r = read(fd, buf + r2, count - r2);
```

Heuristic 2nd Order Buffer Overflow read\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2897
Status	New

The size of the buffer used by myread in r2, at line 50 of mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that myread passes to BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c, to overwrite the target buffer.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Line	57	57
Object	BinaryExpr	r2

Code Snippet
File Name mirror@@dmidecode-dmidecode-3-3-CVE-2023-30630-TP.c
Method static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
57.          r = read(fd, buf + r2, count - r2);
```

Heuristic 2nd Order Buffer Overflow read\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2898
Status	New

The size of the buffer used by myread in count, at line 50 of mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that myread passes to BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c, to overwrite the target buffer.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	57	57
Object	BinaryExpr	count

Code Snippet	
File Name	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method	static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
57.          r = read(fd, buf + r2, count - r2);
```

Heuristic 2nd Order Buffer Overflow read\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2899
Status	New

The size of the buffer used by myread in r2, at line 50 of mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that myread passes to BinaryExpr, at line 50 of mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c, to overwrite the target buffer.

	Source	Destination
File	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Line	57	57
Object	BinaryExpr	r2

Code Snippet	
File Name	mirror@@dmidecode-dmidecode-3-4-CVE-2023-30630-TP.c
Method	static int myread(int fd, u8 *buf, size_t count, const char *prefix)

```
....
57.          r = read(fd, buf + r2, count - r2);
```

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=1020042&projectid=20035&pathid=2647
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c. The application then makes a security decision, error, in michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.13-CVE-2024-35235-TP.c
Line	389	391
Object	getnameinfo	error

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.13-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=1020042&projectid=20035&pathid=2648
Status New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c. The application then makes a security decision, error, in michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.16-CVE-2024-35235-TP.c
Line	389	391
Object	getnameinfo	error

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.16-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 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2649
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 313 of michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c. The application then makes a security decision, error, in michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c line 313, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Line	361	363
Object	getnameinfo	error

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.8-CVE-2024-35235-TP.c
Method httpAddrLookup(

```
....
361.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
363.      if (error)
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2650
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 313 of michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c. The application then makes a security decision, error, in michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c line 313, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c	michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c
Line	361	363
Object	getnameinfo	error

Code Snippet
File Name michaelrsweet@@htmldoc-v1.9.9-CVE-2024-35235-TP.c

Method	httpAddrLookup(

```
....
361.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
363.      if (error)
```

Potential Path Traversal

Query Path:
CPP\Cx\CPP Low Visibility\Potential Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description

Potential Path Traversal\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2550
Status	New

Method main at line 11 of miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 11 of miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	11	75
Object	argv	input_file

Code Snippet	
File Name	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method	int main(int argc, char * * argv) {

```
....
11.  int main(int argc, char * * argv) {
....
75.   fgif = fopen(input_file, "rb");
```

Potential Path Traversal\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2551
Status	New

Method main at line 11 of miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 11 of miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	11	136
Object	argv	tganame

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
11.  int main(int argc, char * * argv) {
....
136.              ftga = fopen(tganame, "wb");
```

Potential Path Traversal\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=2552
Status	New

Method main at line 11 of miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 11 of miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c	miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Line	11	47
Object	argv	argv

Code Snippet
File Name miniupnp@@ngiflib-0.5-CVE-2023-39113-TP.c
Method int main(int argc, char * * argv) {

```
....
11.  int main(int argc, char * * argv) {
....
47.                     log = fopen(argv[i], "w");
```

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=1020042&projectid=20035&pathid=2549
Status	New

	Source	Destination
File	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c	mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c
Line	326	326
Object	getopt	getopt

Code Snippet

File Name mkj@@dropbear-maemo-0.52-2-CVE-2020-36254-FP.c

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

```
....
326.        while ((ch = getopt(argc, argv,
"dfl:prtvBCc:i:P:q1246S:o:F:")) != -1)
```

Improper Resource Shutdown or Release

Query Path:

CPP\Cx\CPP Low Visibility\Improper Resource Shutdown or Release Version:0

Categories

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

Description

Improper Resource Shutdown or Release\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020042&projectid=20035&pathid=3126
Status	New

The application's LogHandler::createLogFile method in MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c defines and initializes the open object at 84. This object encapsulates a limited computing resource, such as open file streams, database connections, or network streams. This resource is not properly closed and released in all situations.

	Source	Destination
File	MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c	MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c
Line	95	95
Object	open	open

Code Snippet
File Name MisterTea@@EternalTerminal-et-v6.2.3-CVE-2022-24950-TP.c
Method string LogHandler::createLogFile(const string &path, const string &filename) {

```
....
95.    FATAL_FAIL(::open(fullFname.c_str(), O_EXCL | O_CREAT, 0600));
```

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

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));
    }
}
```

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 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

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

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;

  void setPassword()
```

```
  {
      password = System.console().readLine("Enter your password: ");
   }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed

{
  private SealedObject password;

  void setPassword()

 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
```

```
	gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
	char* password = (char*) malloc(256);
	int i=0;
	char ch;
	ssize_t k;
	while(k = read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n'){
			password[i]='\0';
			break;
		} else{
			password[i++]=ch;
			fflush(0);
		}
	}
	i=0;
	memset(password,'\0',256);
}

int main()

{

	printf("Please enter a password:\n");
	authfunc();
	somefunc();
	char ch;
	while(read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n')
			break;
	}
}
```

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);
}
```

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;
}
```

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)
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

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

Potential Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
```

```
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

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
```

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

Heuristic 2nd Order Buffer Overflow read

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

Improper Resource Shutdown or Release

Risk

What might happen

Unreleased resources can cause a drain of those available for system use, eventually causing general reliability and availability problems, such as performance degradation, process bloat, and system instability. If a resource leak can be intentionally exploited by an attacker, it may be possible to cause a widespread DoS (Denial of Service) attack. This might even expose sensitive information between unprivileged users, if the resource continues to retain data or user id between subsequent allocations.

Cause

How does it happen

The application code allocates resource objects, but does not ensure these are always closed and released in a timely manner. This can include database connections, file handles, network sockets, or any other resource that needs to be released. In some cases, these might be released - but only if everything works as planned; if there is any runtime exception during the normal course of system operations, resources start to leak.

Note that even in managed-memory languages such as Java, these resources must be explicitly released. Many types of resource are not released even when the Garbage Collector runs; and even if the the object would eventually release the resource, we have no control over when the Garbage Collector does run.

General Recommendations

How to avoid it

- Always close and release all resources.
- Ensure resources are released (along with any other necessary cleanup) in a `finally { }` block. Do not close resources in a `catch { }` block, since this is not ensured to be called.
- Explicitly call .close() on any instance of a class that implements the `Closable` or `AutoClosable` interfaces.
- Alternatively, an even better solution is to use the try-with-resources idiom, in order to automatically close any defined `AutoClosable` instances.

Source Code Examples

Java

Unreleased Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
```

```
}
```

Explicit Release of Database Connection

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try {
            Connection con = DriverManager.getConnection(CONN_STRING);
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
      finally {
            if ((con != null) && (!con.isClosed())) {
            con.close();
         }
     }
}
```

Automatic Implicit Release Using Try-With-Resources

```
private MyObject getDataFromDb(int id)  {
      MyObject data = null;
      Connection con = null;
      try (Connection con = DriverManager.getConnection(CONN_STRING)) {
            data = queryDb(con, id);
      }
      catch ( SQLException e ) {
            handleError(e);
      }
}
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper 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--;
       }
    }
}
```

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

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025