vul_files Scan Report

Project Name	vul_files
Scan Start	Monday, January 6, 2025 2:17:04 PM
Preset	Checkmarx Default
Scan Time	00h:20m:29s
Lines Of Code Scanned	293113
Files Scanned	104
Report Creation Time	Monday, January 6, 2025 3:59:43 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	10/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

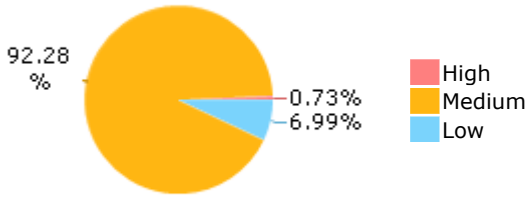
Results Limit

Results limit per query was set to 50

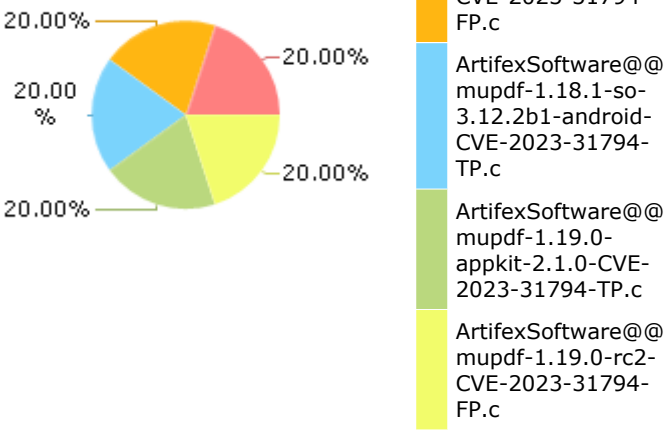
Selected Queries

Selected queries are listed in Result Summary

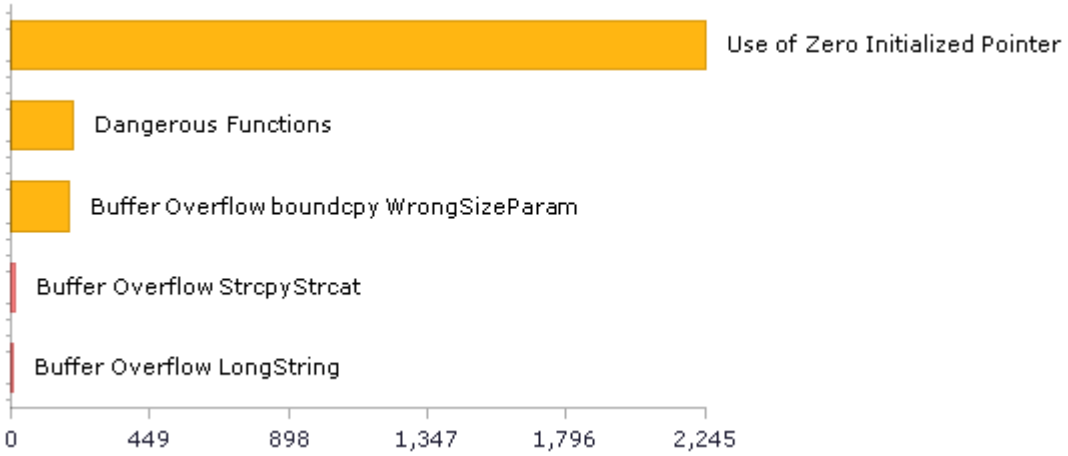
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	275	234
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	41	41
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	13	13
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	203	203
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	8	8
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	203	203
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	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	219	205
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.	0	0
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.	9	9
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	41	41
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.	0	0

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	41	41
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	5	5
SC-4 Information in Shared Resources (P1)	8	8
SC-5 Denial of Service Protection (P1)*	2315	125
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	48	34
SI-11 Error Handling (P2)*	57	57
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	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 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

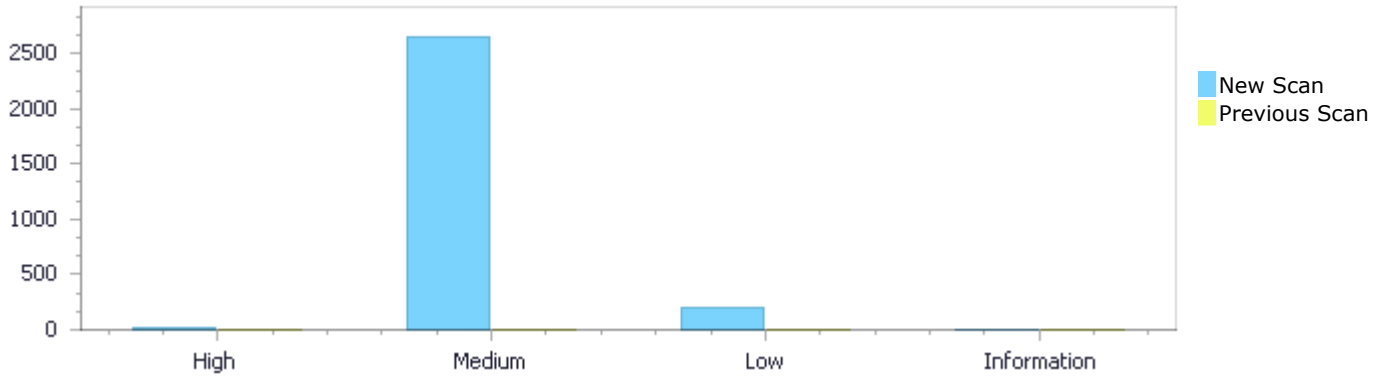
	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, 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	21	2,654	201	0	2,876
Recurrent Issues	0	0	0	0	0
Total	21	2,654	201	0	2,876
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	21	2,654	201	0	2,876
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	21	2,654	201	0	2,876

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	15	High
Buffer Overflow LongString	6	High
Use of Zero Initialized Pointer	2246	Medium
Dangerous Functions	203	Medium
Buffer Overflow boundcpy WrongSizeParam	189	Medium

Heap Inspection	8	Medium
Memory Leak	4	Medium
MemoryFree on StackVariable	4	Medium
Unchecked Return Value	57	Low
NULL Pointer Dereference	56	Low
Improper Resource Access Authorization	41	Low
Unchecked Array Index	18	Low
Arithmenic Operation On Boolean	9	Low
Heuristic 2nd Order Buffer Overflow read	9	Low
Use of Sizeof On a Pointer Type	6	Low
Use of Insufficiently Random Values	5	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	310
ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	310
ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	310
ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	310
ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	310
ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	303
ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	188
ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	188
arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	23
arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	23

Scan Results Details

Buffer Overflow StrcpyStrcat

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=7
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in ClientPortPtr, at line 35 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	35	58
Object	aRequest	ClientPortPtr

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
58.              strcpy(CP,ClientPortPtr);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=8
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in CP, at line 35 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	CP

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=9
Status New

The size of the buffer used by CRtspSession::ParseRtspRequest in pCP, at line 35 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	pCP

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=10
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in ClientPortPtr, at line 35 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	35	58
Object	aRequest	ClientPortPtr

Code Snippet

File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c

Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
58.              strcpy(CP,ClientPortPtr);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=11
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in CP, at line 35 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	CP

Code Snippet

File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c

Method	bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=12
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in pCP, at line 35 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	pCP

Code Snippet

File Name	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method	bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=13
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in ClientPortPtr, at line 35 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination

File	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	35	58
Object	aRequest	ClientPortPtr

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
58.              strcpy(CP,ClientPortPtr);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=14
Status New

The size of the buffer used by CRtspSession::ParseRtspRequest in CP, at line 35 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	CP

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=15
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in pCP, at line 35 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	pCP

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=16
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in ClientPortPtr, at line 35 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	35	58
Object	aRequest	ClientPortPtr

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
58.              strcpy(CP,ClientPortPtr);
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=17
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in CP, at line 35 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	CP

Code Snippet

File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c

Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=18
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in pCP, at line 35 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c

Line	35	63
Object	aRequest	pCP

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=19
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in ClientPortPtr, at line 35 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	35	58
Object	aRequest	ClientPortPtr

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
58.              strcpy(CP,ClientPortPtr);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=20
Status	New

The size of the buffer used by CRtspSession::ParseRtspRequest in CP, at line 35 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	CP

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=21
Status New

The size of the buffer used by CRtspSession::ParseRtspRequest in pCP, at line 35 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CRtspSession::ParseRtspRequest passes to aRequest, at line 35 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	35	63
Object	aRequest	pCP

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
35.  bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned
aRequestSize)
....
63.                  strcpy(CP,pCP);
```

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=1000007&projectid=1&pathid=1
Status	New

The size of the buffer used by ExecuteActionVocbase in args, at line 1002 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TRI_RequestCppToV8 passes to "http", at line 313 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	395	1026
Object	"http"	args

Code Snippet

File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c

Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
395.      req->Set(context, ProtocolKey, TRI_V8_ASCII_STRING(isolate,
"http")).FromMaybe(false);
```

File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c

Method static TRI_action_result_t ExecuteActionVocbase(TRI_vocbase_t* vocbase, v8::Isolate* isolate,

```
....
1026.    v8::Handle<v8::Value> args[2] = {req, res};
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2
Status	New

The size of the buffer used by ExecuteActionVocbase in args, at line 1002 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TRI_RequestCppToV8 passes to "vst", at line 313 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	397	1026
Object	"vst"	args

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
397.      req->Set(context, ProtocolKey, TRI_V8_ASCII_STRING(isolate,
"vst")).FromMaybe(false);
```

File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c

Method static TRI_action_result_t ExecuteActionVocbase(TRI_vocbase_t* vocbase, v8::Isolate* isolate,

```
....
1026.    v8::Handle<v8::Value> args[2] = {req, res};
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=3
Status	New

The size of the buffer used by ExecuteActionVocbase in args, at line 1002 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TRI_RequestCppToV8 passes to "internals", at line 313 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	431	1026
Object	"internals"	args

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
431.    req->Set(context, TRI_V8_ASCII_STRING(isolate, "internals"),
v8::External::New(isolate, request)).FromMaybe(false);
```

File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c

Method static TRI_action_result_t ExecuteActionVocbase(TRI_vocbase_t* vocbase, v8::Isolate* isolate,

```
....
1026.    v8::Handle<v8::Value> args[2] = {req, res};
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=4
Status	New

The size of the buffer used by ExecuteActionVocbase in args, at line 1002 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TRI_RequestCppToV8 passes to "http", at line 313 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	395	1026
Object	"http"	args

Code Snippet

File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c

Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
395.      req->Set(context, ProtocolKey, TRI_V8_ASCII_STRING(isolate,
"http")).FromMaybe(false);
```

File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c

Method static TRI_action_result_t ExecuteActionVocbase(TRI_vocbase_t* vocbase, v8::Isolate* isolate,

```
....
1026.    v8::Handle<v8::Value> args[2] = {req, res};
```

Buffer Overflow LongString\Path 5:

Severity High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=5
Status	New

The size of the buffer used by ExecuteActionVocbase in args, at line 1002 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TRI_RequestCppToV8 passes to "vst", at line 313 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	397	1026
Object	"vst"	args

Code Snippet

File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c

Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
397.      req->Set(context, ProtocolKey, TRI_V8_ASCII_STRING(isolate,
"vst")).FromMaybe(false);
```

File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c

Method static TRI_action_result_t ExecuteActionVocbase(TRI_vocbase_t* vocbase, v8::Isolate* isolate,

```
....
1026.    v8::Handle<v8::Value> args[2] = {req, res};
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=6
Status	New

The size of the buffer used by ExecuteActionVocbase in args, at line 1002 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TRI_RequestCppToV8 passes to "internals", at line 313 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	431	1026
Object	"internals"	args

Code Snippet	
File Name	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method	v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
431.    req->Set(context, TRI_V8_ASCII_STRING(isolate, "internals"),
v8::External::New(isolate, request)).FromMaybe(false);
```

File Name	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method	static TRI_action_result_t ExecuteActionVocbase(TRI_vocbase_t* vocbase, v8::Isolate* isolate,

```
....
1026.    v8::Handle<v8::Value> args[2] = {req, res};
```

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=1000007&projectid=1&pathid=448
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	542	571
Object	paint	pattern

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method	gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
542.                            paint = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=449
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	517	571
Object	paint	pattern

Code Snippet

File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c

Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
517.                pdf_obj *paint = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=450
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c

Line	549	572
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
549.                            tiling = NULL;
....
572.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=451
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	518	572
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
518.                pdf_obj *tiling = NULL;
....
572.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=452
Status	New

The variable declared in shading at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	519	573
Object	shading	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
519.              pdf_obj *shading = NULL;
....
573.              glo->pattern[glo->patterns - 1].u.pattern.shading =
shading;
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=453
Status New

The variable declared in cs at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by cs at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	726	807
Object	cs	cs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *cs = NULL;
....
807.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

Use of Zero Initialized Pointer\Path 7:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=454
Status	New

The variable declared in altcs at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by altcs at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	727	809
Object	altcs	altcs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
727.                    char *altcs = NULL;
....
809.                          glo->image[i].u.image.altcs ? altcs : "",
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=455
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	542	571
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
542.                            paint = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=456
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	517	571
Object	paint	pattern

Code Snippet

File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c

Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
517.                pdf_obj *paint = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=457
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c

Line	549	572
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
549.                            tiling = NULL;
....
572.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=458
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	518	572
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
518.                pdf_obj *tiling = NULL;
....
572.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=459
Status	New

The variable declared in shading at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 508.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	519	573
Object	shading	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
519.                pdf_obj *shading = NULL;
....
573.                glo->pattern[glo->patterns - 1].u.pattern.shading =
shading;
```

Use of Zero Initialized Pointer\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=460
Status New

The variable declared in cs at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by cs at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	726	807
Object	cs	cs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *cs = NULL;
....
807.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

Use of Zero Initialized Pointer\Path 14:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=461
Status	New

The variable declared in altcs at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by altcs at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	727	809
Object	altcs	altcs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
727.                    char *altcs = NULL;
....
809.                          glo->image[i].u.image.altcs ? altcs : "",
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=462
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	541	570
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
541.                            paint = NULL;
....
570.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=463
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	516	570
Object	paint	pattern

Code Snippet

File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c

Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
516.                pdf_obj *paint = NULL;
....
570.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=464
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c

Line	548	571
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
548.                            tiling = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=465
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	517	571
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
517.                pdf_obj *tiling = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=466
Status	New

The variable declared in shading at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	518	572
Object	shading	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
518.                pdf_obj *shading = NULL;
....
572.                glo->pattern[glo->patterns - 1].u.pattern.shading =
shading;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=467
Status	New

The variable declared in cs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679 is not initialized when it is used by cs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	725	806
Object	cs	cs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
725.                    char *cs = NULL;
....
806.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=468
Status	New

The variable declared in altcs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679 is not initialized when it is used by altcs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	726	808
Object	altcs	altcs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *altcs = NULL;
....
808.                          glo->image[i].u.image.altcs ? altcs : "",
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=469
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	541	570
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
541.                            paint = NULL;
....
570.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=470
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	516	570
Object	paint	pattern

Code Snippet

File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c

Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
516.                pdf_obj *paint = NULL;
....
570.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=471
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c

Line	548	571
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
548.                            tiling = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=472
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	517	571
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
517.                pdf_obj *tiling = NULL;
....
571.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=473
Status	New

The variable declared in shading at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 507.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	518	572
Object	shading	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
518.                pdf_obj *shading = NULL;
....
572.                glo->pattern[glo->patterns - 1].u.pattern.shading =
shading;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=474
Status	New

The variable declared in cs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679 is not initialized when it is used by cs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	725	806
Object	cs	cs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
725.                    char *cs = NULL;
....
806.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=475
Status	New

The variable declared in altcs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679 is not initialized when it is used by altcs at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	726	808
Object	altcs	altcs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *altcs = NULL;
....
808.                          glo->image[i].u.image.altcs ? altcs : "",
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=476
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	563	592
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
563.                            paint = NULL;
....
592.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=477
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	538	592
Object	paint	pattern

Code Snippet

File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c

Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
538.                pdf_obj *paint = NULL;
....
592.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=478
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c

Line	570	593
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
570.                            tiling = NULL;
....
593.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=479
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	539	593
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
539.                pdf_obj *tiling = NULL;
....
593.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=480
Status	New

The variable declared in shading at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	540	594
Object	shading	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
540.                pdf_obj *shading = NULL;
....
594.                glo->pattern[glo->patterns - 1].u.pattern.shading =
shading;
```

Use of Zero Initialized Pointer\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=481
Status New

The variable declared in cs at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701 is not initialized when it is used by cs at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	747	828
Object	cs	cs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
747.                    char *cs = NULL;
....
828.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=482
Status	New

The variable declared in altcs at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701 is not initialized when it is used by altcs at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	748	830
Object	altcs	altcs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
748.                    char *altcs = NULL;
....
830.                          glo->image[i].u.image.altcs ? altcs : "",
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=483
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	563	592
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
563.                            paint = NULL;
....
592.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=484
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	538	592
Object	paint	pattern

Code Snippet

File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c

Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
538.                pdf_obj *paint = NULL;
....
592.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=485
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c

Line	570	593
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
570.                            tiling = NULL;
....
593.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=486
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	539	593
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
539.                pdf_obj *tiling = NULL;
....
593.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=487
Status	New

The variable declared in shading at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	540	594
Object	shading	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
540.                pdf_obj *shading = NULL;
....
594.                glo->pattern[glo->patterns - 1].u.pattern.shading =
shading;
```

Use of Zero Initialized Pointer\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=488
Status New

The variable declared in cs at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701 is not initialized when it is used by cs at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	747	828
Object	cs	cs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
747.                    char *cs = NULL;
....
828.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

Use of Zero Initialized Pointer\Path 42:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=489
Status	New

The variable declared in altcs at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701 is not initialized when it is used by altcs at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	748	830
Object	altcs	altcs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
748.                    char *altcs = NULL;
....
830.                          glo->image[i].u.image.altcs ? altcs : "",
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=490
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	563	592
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
563.                            paint = NULL;
....
592.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=491
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	538	592
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
538.                pdf_obj *paint = NULL;
....
592.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=492
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c

Line	570	593
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
570.                            tiling = NULL;
....
593.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=493
Status	New

The variable declared in tiling at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	539	593
Object	tiling	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
539.                pdf_obj *tiling = NULL;
....
593.                glo->pattern[glo->patterns - 1].u.pattern.tiling =
tiling;
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=494
Status	New

The variable declared in shading at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	540	594
Object	shading	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
540.              pdf_obj *shading = NULL;
....
594.              glo->pattern[glo->patterns - 1].u.pattern.shading =
shading;
```

Use of Zero Initialized Pointer\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=495
Status New

The variable declared in cs at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703 is not initialized when it is used by cs at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	749	830
Object	cs	cs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
749.                    char *cs = NULL;
....
830.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

Use of Zero Initialized Pointer\Path 49:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=496
Status	New

The variable declared in altcs at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703 is not initialized when it is used by altcs at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	750	832
Object	altcs	altcs

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
750.                    char *altcs = NULL;
....
832.                          glo->image[i].u.image.altcs ? altcs : "",
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=497
Status	New

The variable declared in paint at ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c in line 529 is not initialized when it is used by pattern at ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c in line 529.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	563	592
Object	paint	pattern

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method gatherpatterns(fz_context *ctx, globals *glo, int page, pdf_obj *pageref, pdf_obj *dict)

```
....
563.                            paint = NULL;
....
592.                glo->pattern[glo->patterns - 1].u.pattern.paint =
paint;
```

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=1000007&projectid=1&pathid=211
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Line	494	494
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
494.        memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=212
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Method int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.       memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=213
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Line	494	494
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
494.         memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=214
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Method int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.      memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=215
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Line	494	494
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
494.        memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 6:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=216
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Method int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.       memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=217
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Line	494	494
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
494.         memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=218
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Method int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.      memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=219
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Line	494	494
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
494.        memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=220
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Method int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.      memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=221
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Line	494	494
Object	memcpy	memcpy

Code Snippet	
File Name	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Method	static int session_new(nghttp2_session **session_ptr,

```
....
494.        memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=222
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet	
File Name	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Method	int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.      memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=223
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Line	494	494

Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
494.        memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=224
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Method int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.      memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=225
Status	New

The dangerous function, memcpy, was found in use at line 403 in arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-	arangodb@@arangodb-v3.9.6-CVE-

	2024-28182-TP.c	2024-28182-TP.c
Line	494	494
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
494.        memcpy((*session_ptr)->user_recv_ext_types, option-
>user_recv_ext_types,
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=226
Status	New

The dangerous function, memcpy, was found in use at line 6899 in arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Line	6923	6923
Object	memcpy	memcpy

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Method int nghttp2_session_add_goaway(nghttp2_session *session, int32_t last_stream_id,

```
....
6923.      memcpy(opaque_data_copy, opaque_data, opaque_data_len);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=227
Status	New

The dangerous function, memcpy, was found in use at line 35 in arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	43	43
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
43.      memcpy(CurRequest,aRequest,aRequestSize);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=228
Status	New

The dangerous function, memcpy, was found in use at line 73 in arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	96	96
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method int op_test(OpusHead *_head,

```
....
96.      memcpy(data,_initial_data,_initial_bytes);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=229
Status	New

The dangerous function, memcpy, was found in use at line 1358 in arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1387.       memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=230
Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1457	1457
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1457.     memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=231

Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1469	1469
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1469.     memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=232
Status	New

The dangerous function, memcpy, was found in use at line 1519 in arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1545	1545
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1545.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=233
Status	New

The dangerous function, memcpy, was found in use at line 2827 in arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	2849	2849
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2849.            memcpy(_pcm,_of->od_buffer+nchannels*od_buffer_pos,
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=234
Status	New

The dangerous function, memcpy, was found in use at line 3060 in arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	3064	3064
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3064.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Dangerous Functions\Path 25:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=235
Status	New

The dangerous function, memcpy, was found in use at line 35 in arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	43	43
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
43.      memcpy(CurRequest,aRequest,aRequestSize);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=236
Status	New

The dangerous function, memcpy, was found in use at line 73 in arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	96	96
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method int op_test(OpusHead *_head,

```
....
96.      memcpy(data,_initial_data,_initial_bytes);
```

Dangerous Functions\Path 27:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=237
Status	New

The dangerous function, memcpy, was found in use at line 1358 in arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1387.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=238
Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	1457	1457
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1457.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=239
Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	1469	1469
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1469.     memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=240
Status	New

The dangerous function, memcpy, was found in use at line 1519 in arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	1545	1545
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1545.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=241
Status	New

The dangerous function, memcpy, was found in use at line 2827 in arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	2849	2849
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2849.            memcpy(_pcm,_of->od_buffer+nchannels*od_buffer_pos,
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=242
Status	New

The dangerous function, memcpy, was found in use at line 3060 in arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	3064	3064
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3064.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=243
Status	New

The dangerous function, memcpy, was found in use at line 35 in arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	43	43
Object	memcpy	memcpy

Code Snippet

File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c

Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
43.      memcpy(CurRequest,aRequest,aRequestSize);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=244
Status	New

The dangerous function, memcpy, was found in use at line 73 in arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	96	96
Object	memcpy	memcpy

Code Snippet

File Name	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method	int op_test(OpusHead *_head,

```
....
96.      memcpy(data,_initial_data,_initial_bytes);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=245
Status	New

The dangerous function, memcpy, was found in use at line 1358 in arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet

File Name	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method	static int op_make_decode_ready(OggOpusFile *_of){

```
....
1387.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=246
Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	1457	1457
Object	memcpy	memcpy

Code Snippet	
File Name	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method	static int op_open_seekable2(OggOpusFile *_of){

```
....
1457.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=247
Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	1469	1469
Object	memcpy	memcpy

Code Snippet	
File Name	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method	static int op_open_seekable2(OggOpusFile *_of){

```
....
1469.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=248
Status	New

The dangerous function, memcpy, was found in use at line 1519 in arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	1545	1545

Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1545.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=249
Status	New

The dangerous function, memcpy, was found in use at line 2827 in arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	2849	2849
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2849.            memcpy(_pcm,_of->od_buffer+nchannels*od_buffer_pos,
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=250
Status	New

The dangerous function, memcpy, was found in use at line 3060 in arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c

Line	3064	3064
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3064.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=251
Status	New

The dangerous function, memcpy, was found in use at line 73 in arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	96	96
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method int op_test(OpusHead *_head,

```
....
96.      memcpy(data,_initial_data,_initial_bytes);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=252
Status	New

The dangerous function, memcpy, was found in use at line 1358 in arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-	arendst@@Tasmota-v12.2.0-CVE-2022-

	47021-TP.c	47021-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1387.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=253
Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	1457	1457
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1457.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=254
Status	New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	1469	1469
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1469.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=255
Status	New

The dangerous function, memcpy, was found in use at line 1519 in arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	1545	1545
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1545.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=256
Status	New

The dangerous function, memcpy, was found in use at line 2827 in arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	2849	2849
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2849.            memcpy(_pcm,_of->od_buffer+nchannels*od_buffer_pos,
```

Dangerous Functions\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=257
Status New

The dangerous function, memcpy, was found in use at line 3060 in arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	3064	3064
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3064.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Dangerous Functions\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=258
Status New

The dangerous function, memcpy, was found in use at line 73 in arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	96	96
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method int op_test(OpusHead *_head,

```
....
96.      memcpy(data,_initial_data,_initial_bytes);
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=259
Status New

The dangerous function, memcpy, was found in use at line 1358 in arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1387.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=260
Status New

The dangerous function, memcpy, was found in use at line 1431 in arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	1457	1457
Object	memcpy	memcpy

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1457.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

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=1000007&projectid=1&pathid=22
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=23
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Method static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=24
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c

Method	static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=25
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet

File Name	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Method	static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=26
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet

File Name	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Method	static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=27
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet

File Name	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Method	static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=28
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet	
File Name	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Method	static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=29
Status	New

The size of the buffer used by session_new in session_ptr, at line 403 of arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_new passes to session_ptr, at line 403 of arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

Code Snippet	
File Name	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Method	static int session_new(nghttp2_session **session_ptr,

```
....
495.                sizeof((*session_ptr)->user_recv_ext_types));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=30
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	243	243
Object	fz_rect	fz_rect

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method	gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
243.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=31
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	243	243
Object	fz_rect	fz_rect

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method	gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
243.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=32
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c

Line	242	242
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
242.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=33
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	242	242
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
242.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=34
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	264	264
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
264.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=35
Status New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	264	264
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
264.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=36
Status New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	264	264
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
264.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=37
Status New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	264	264
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
264.        memcpy(glo->dim[glo->dims - 1].u.dim.bbox, &bbox, sizeof
(fz_rect));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=38
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=39
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=40
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=41
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=42
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=43
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet	
File Name	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Method	static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=44
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet	
File Name	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Method	static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=45
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-	arangodb@@arangodb-v3.8.3-

	preview.3-CVE-2024-28182-TP.c	preview.3-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=46
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=47
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset

passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=48
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=49
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=50
Status New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=51
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=52
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_frame, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
363.    memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=53
Status	New

The size of the buffer used by session_inbound_frame_reset in nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_inbound_frame_reset passes to nghttp2_ext_frame_payload, at line 298 of arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Method static void session_inbound_frame_reset(nghttp2_session *session) {

```
....
364.    memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=54
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	230	230
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
230.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=55
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 207 of ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	230	230
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
230.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=56
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	229	229
Object	fz_rect	fz_rect

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method	gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
229.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=57
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 206 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	229	229
Object	fz_rect	fz_rect

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method	gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
229.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=58
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	251	251

Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
251.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=59
Status New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	251	251
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
251.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=60
Status New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c, to overwrite the target buffer.

	Source	Destination

File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	251	251
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
251.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=61
Status	New

The size of the buffer used by gatherdimensions in fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gatherdimensions passes to fz_rect, at line 228 of ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c, to overwrite the target buffer.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	251	251
Object	fz_rect	fz_rect

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method gatherdimensions(fz_context *ctx, globals *glo, int page, pdf_obj *pageref)

```
....
251.                if (!memcmp(glo->dim[j].u.dim.bbox, &bbox, sizeof
(fz_rect)))
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=62
Status	New

The size of the buffer used by op_make_decode_ready in channel_count, at line 1358 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that op_make_decode_ready passes to channel_count, at line 1358 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1387	1387
Object	channel_count	channel_count

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1387.       memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=63
Status	New

The size of the buffer used by op_make_decode_ready in head, at line 1358 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_make_decode_ready passes to head, at line 1358 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1387	1387
Object	head	head

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1387.       memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=64
Status	New

The size of the buffer used by op_open_seekable2 in start_op_count, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to start_op_count, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1457	1457
Object	start_op_count	start_op_count

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1457.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=65
Status New

The size of the buffer used by op_open_seekable2 in op_start, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to op_start, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1457	1457
Object	op_start	op_start

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1457.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=66

Status	New

The size of the buffer used by op_open_seekable2 in start_op_count, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to start_op_count, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1469	1469
Object	start_op_count	start_op_count

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1469.     memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=67
Status	New

The size of the buffer used by op_open_seekable2 in _of, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to _of, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1469	1469
Object	_of	_of

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1469.     memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=68
Status	New

The size of the buffer used by op_open1 in _initial_bytes, at line 1519 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open1 passes to _initial_bytes, at line 1519 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1545	1545
Object	_initial_bytes	_initial_bytes

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1545.       memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=69
Status	New

The size of the buffer used by op_open1 in buffer, at line 1519 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open1 passes to buffer, at line 1519 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1545	1545
Object	buffer	buffer

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open1(OggOpusFile *_of,

```
....
1545.       memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=70
Status	New

The size of the buffer used by op_stereo_filter in _nsamples, at line 3060 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_stereo_filter passes to _nsamples, at line 3060 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	3064	3064
Object	_nsamples	_nsamples

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3064.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=71
Status	New

The size of the buffer used by op_stereo_filter in _src, at line 3060 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_stereo_filter passes to _src, at line 3060 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	3064	3064
Object	_src	_src

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3064.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

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=1000007&projectid=1&pathid=436
Status	New

Method pdfinfo_main at line 1005 of ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	1008	1008
Object	password	password

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1008.       char *password = "";
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=437
Status	New

Method pdfinfo_main at line 1005 of ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	1008	1008
Object	password	password

Code Snippet

File Name	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method	int pdfinfo_main(int argc, char **argv)

```
....
1008.       char *password = "";
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=438
Status	New

Method pdfinfo_main at line 1007 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	1010	1010
Object	password	password

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method	int pdfinfo_main(int argc, char **argv)

```
....
1010.       char *password = "";
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=439
Status	New

Method pdfinfo_main at line 1007 of ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	1010	1010
Object	password	password

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c

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

```
....
1010.       char *password = "";
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=440
Status	New

Method pdfinfo_main at line 1029 of ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	1032	1032
Object	password	password

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method	int pdfinfo_main(int argc, char **argv)

```
....
1032.       char *password = "";
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=441
Status	New

Method pdfinfo_main at line 1029 of ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	1032	1032
Object	password	password

Code Snippet	
File Name	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method	int pdfinfo_main(int argc, char **argv)

```
....
1032.       char *password = "";
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=442
Status	New

Method pdfinfo_main at line 1031 of ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	1034	1034
Object	password	password

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1034.       char *password = "";
```

Heap Inspection\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=443
Status	New

Method pdfinfo_main at line 1019 of ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	1022	1022
Object	password	password

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1022.       char *password = "";
```

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=1000007&projectid=1&pathid=414
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=415
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=416
Status New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file arangodb@@arangodb-v3.9.10-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.9.10-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-14397-FP.c
Method intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=417
Status New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file arangodb@@arangodb-v3.9.6-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.9.6-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

Code Snippet

File Name	arangodb@@arangodb-v3.9.6-CVE-2020-14397-FP.c
Method	intern_array (unw_addr_space_t as, unw_accessors_t *a,

```
....
122.      free (data);
```

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=1000007&projectid=1&pathid=444
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet

File Name	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-14397-FP.c
Method	intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=445
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=446
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.9.10-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=447
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-14397-FP.c	arangodb@@arangodb-v3.9.6-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2020-14397-FP.c
Method intern_regions (unw_addr_space_t as, unw_accessors_t *a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

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=1000007&projectid=1&pathid=2740
Status	New

The CRtspSession::Handle_RtspOPTION method calls the snprintf function, at line 231 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	235	235
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspOPTION()

```
....
235.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2741
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	254	254

Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
254.          snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2742
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	270	270
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
270.      snprintf(SDPBuf,sizeof(SDPBuf),
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2743
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c

Line	286	286
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
286.      snprintf(URLBuf,sizeof(URLBuf),
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2744
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	290	290
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
290.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2745
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-	arendst@@Tasmota-v10.0.0-CVE-2022-

	43294-TP.c	43294-TP.c
Line	316	316
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
316.
snprintf(Transport,sizeof(Transport),"RTP/AVP/TCP;unicast;interleaved=0-
1");
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2746
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	318	318
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
318.          snprintf(Transport,sizeof(Transport),
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2747
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	324	324
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
324.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2748
Status New

The CRtspSession::Handle_RtspPLAY method calls the snprintf function, at line 337 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	342	342
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspPLAY()

```
....
342.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2749
Status New

The CRtspSession::Handle_RtspOPTION method calls the snprintf function, at line 231 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	235	235
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspOPTION()

```
....
235.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2750
Status New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	254	254
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
254.          snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2751
Status New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	270	270
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
270.      snprintf(SDPBuf,sizeof(SDPBuf),
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2752
Status New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	286	286
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
286.      snprintf(URLBuf,sizeof(URLBuf),
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2753
Status New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	290	290
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
290.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2754
Status New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	316	316
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
316.
snprintf(Transport,sizeof(Transport),"RTP/AVP/TCP;unicast;interleaved=0-1");
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2755
Status New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	318	318
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
318.          snprintf(Transport,sizeof(Transport),
```

Unchecked Return Value\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2756
Status New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	324	324
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
324.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2757
Status New

The CRtspSession::Handle_RtspPLAY method calls the snprintf function, at line 337 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	342	342
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspPLAY()

```
....
342.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2758
Status New

The CRtspSession::Handle_RtspOPTION method calls the snprintf function, at line 231 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	235	235
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspOPTION()

```
....
235.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2759

Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	254	254
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
254.          snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2760
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	270	270
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
270.      snprintf(SDPBuf,sizeof(SDPBuf),
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=2761
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	286	286
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
286.      snprintf(URLBuf,sizeof(URLBuf),
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2762
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	290	290
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
290.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2763
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	316	316
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
316.
snprintf(Transport,sizeof(Transport),"RTP/AVP/TCP;unicast;interleaved=0-1");
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2764
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	318	318
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
318.          snprintf(Transport,sizeof(Transport),
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2765
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	324	324
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
324.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2766
Status	New

The CRtspSession::Handle_RtspPLAY method calls the snprintf function, at line 337 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	342	342
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspPLAY()

```
....
342.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2767
Status	New

The CRtspSession::Handle_RtspOPTION method calls the snprintf function, at line 231 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	235	235
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspOPTION()

```
....
235.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2768
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	254	254
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
254.          snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2769
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	270	270
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
270.      snprintf(SDPBuf,sizeof(SDPBuf),
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2770
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	286	286
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
286.      snprintf(URLBuf,sizeof(URLBuf),
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2771
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	290	290
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
290.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2772
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	316	316
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c

Method	void CRtspSession::Handle_RtspSETUP()

```
....
316.
snprintf(Transport,sizeof(Transport),"RTP/AVP/TCP;unicast;interleaved=0-
1");
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2773
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	318	318
Object	snprintf	snprintf

Code Snippet	
File Name	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method	void CRtspSession::Handle_RtspSETUP()

```
....
318.          snprintf(Transport,sizeof(Transport),
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2774
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	324	324
Object	snprintf	snprintf

Code Snippet	
File Name	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method	void CRtspSession::Handle_RtspSETUP()

```
....
324.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2775
Status	New

The CRtspSession::Handle_RtspPLAY method calls the snprintf function, at line 337 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	342	342
Object	snprintf	snprintf

Code Snippet	
File Name	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method	void CRtspSession::Handle_RtspPLAY()

```
....
342.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2776
Status	New

The CRtspSession::Handle_RtspOPTION method calls the snprintf function, at line 231 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	235	235

Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspOPTION()

```
....
235.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2777
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	254	254
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
254.          snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2778
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c

Line	270	270
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
270.      snprintf(SDPBuf,sizeof(SDPBuf),
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2779
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	286	286
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
286.      snprintf(URLBuf,sizeof(URLBuf),
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2780
Status	New

The CRtspSession::Handle_RtspDESCRIBE method calls the snprintf function, at line 242 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-	arendst@@Tasmota-v9.5.0-CVE-2022-

	43294-TP.c	43294-TP.c
Line	290	290
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
290.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2781
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	316	316
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
316.
snprintf(Transport,sizeof(Transport),"RTP/AVP/TCP;unicast;interleaved=0-1");
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2782
Status	New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	318	318
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
318.          snprintf(Transport,sizeof(Transport),
```

Unchecked Return Value\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2783
Status New

The CRtspSession::Handle_RtspSETUP method calls the snprintf function, at line 306 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	324	324
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspSETUP()

```
....
324.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2784
Status New

The CRtspSession::Handle_RtspPLAY method calls the snprintf function, at line 337 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	342	342
Object	snprintf	snprintf

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspPLAY()

```
....
342.      snprintf(Response,sizeof(Response),
```

Unchecked Return Value\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2785
Status New

The op_open_seekable2_impl method calls the sr function, at line 1402 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-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	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1406	1406
Object	sr	sr

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
```

Unchecked Return Value\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2786
Status New

The op_open_seekable2 method calls the os_start function, at line 1431 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-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	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1433	1433
Object	os_start	os_start

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1433.    ogg_stream_state  *os_start =
(ogg_stream_state*)malloc(sizeof(ogg_stream_state));
```

Unchecked Return Value\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2787
Status New

The op_open_seekable2_impl method calls the sr function, at line 1402 of arendst@@Tasmota-v11.0.0-CVE-2022-47021-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	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	1406	1406
Object	sr	sr

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
```

Unchecked Return Value\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=2788
Status	New

The op_open_seekable2 method calls the os_start function, at line 1431 of arendst@@Tasmota-v11.0.0-CVE-2022-47021-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	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	1433	1433
Object	os_start	os_start

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1433.    ogg_stream_state  *os_start =
(ogg_stream_state*)malloc(sizeof(ogg_stream_state));
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2789
Status	New

The op_open_seekable2_impl method calls the sr function, at line 1402 of arendst@@Tasmota-v12.0.0-CVE-2022-47021-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	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	1406	1406
Object	sr	sr

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
```

NULL Pointer Dereference

Query Path:

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=1000007&projectid=1&pathid=2803
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	726	807
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *cs = NULL;
....
807.                            glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2804
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	727	809

Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
727.                    char *altcs = NULL;
....
809.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2805
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	726	807
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *cs = NULL;
....
807.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2806
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c in line 680.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	727	809
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
727.                    char *altcs = NULL;
....
809.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2807
Status New

The variable declared in null at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	725	806
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
725.                    char *cs = NULL;
....
806.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2808
Status New

The variable declared in null at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	726	808
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *altcs = NULL;
....
808.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2809
Status New

The variable declared in null at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	725	806
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
725.                    char *cs = NULL;
....
806.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 8:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2810
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c in line 679.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	726	808
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
726.                    char *altcs = NULL;
....
808.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2811
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	747	828
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
747.                    char *cs = NULL;
....
828.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2812
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	748	830
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
748.                    char *altcs = NULL;
....
830.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2813
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	747	828

Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
747.                    char *cs = NULL;
....
828.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2814
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c in line 701.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	748	830
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
748.                    char *altcs = NULL;
....
830.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2815
Status	New

The variable declared in null at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	749	830
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
749.                    char *cs = NULL;
....
830.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2816
Status New

The variable declared in null at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c in line 703.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	750	832
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
750.                    char *altcs = NULL;
....
832.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2817
Status New

The variable declared in null at ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c in line 691 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c in line 691.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	737	818
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
737.                    char *cs = NULL;
....
818.                          glo->image[i].u.image.cs ? cs :
"ImageMask",
```

NULL Pointer Dereference\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2818
Status New

The variable declared in null at ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c in line 691 is not initialized when it is used by image at ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c in line 691.

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	738	820
Object	null	image

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method printinfo(fz_context *ctx, globals *glo, char *filename, int show, int page)

```
....
738.                    char *altcs = NULL;
....
820.                          glo->image[i].u.image.altcs ? altcs : "",
```

NULL Pointer Dereference\Path 17:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2819
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	654
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
654.      rawSuffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
rawSuffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2820
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by rawSuffixArray at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	654
Object	0	rawSuffixArray

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
654.      rawSuffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
rawSuffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2821
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	664
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
664.    req->Set(context, RawSuffixKey,
rawSuffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2822
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by req at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	668
Object	0	req

Code Snippet	
File Name	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method	v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
668.    req->Set(context, PathKey, TRI_V8_STD_STRING(isolate,
path)).FromMaybe(false);
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2823
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by req at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	662
Object	0	req

Code Snippet	
File Name	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method	v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
662.    req->Set(context, SuffixKey, suffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2824
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by req at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c

Line	643	664
Object	0	req

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
664.    req->Set(context, RawSuffixKey,
rawSuffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2825
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	662
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
662.    req->Set(context, SuffixKey, suffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2826
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	668
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
668.    req->Set(context, PathKey, TRI_V8_STD_STRING(isolate,
path)).FromMaybe(false);
```

NULL Pointer Dereference\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2827
Status New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	653
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
653.      suffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
suffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2828
Status New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by suffixArray at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	643	653
Object	0	suffixArray

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
653.      suffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
suffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2829
Status New

The variable declared in 0 at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 1291 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c in line 1291.

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	1372	1448
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method static void JS_RequestParts(v8::FunctionCallbackInfo<v8::Value> const& args) {

```
....
1372.        uint32_t j = 0;
....
1448.          result->Set(context, j++, partObject).FromMaybe(false);
```

NULL Pointer Dereference\Path 28:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2830
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	654
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
654.      rawSuffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
rawSuffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2831
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by rawSuffixArray at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	654
Object	0	rawSuffixArray

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
654.      rawSuffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
rawSuffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2832
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	664
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
664.    req->Set(context, RawSuffixKey,
rawSuffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2833
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by req at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	668

Object	0	req

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
668.    req->Set(context, PathKey, TRI_V8_STD_STRING(isolate,
path)).FromMaybe(false);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2834
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by req at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	662
Object	0	req

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
662.    req->Set(context, SuffixKey, suffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2835
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by req at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	664
Object	0	req

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
664.    req->Set(context, RawSuffixKey,
rawSuffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2836
Status New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	662
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
662.    req->Set(context, SuffixKey, suffixArray).FromMaybe(false);
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2837
Status New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	668
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
668.    req->Set(context, PathKey, TRI_V8_STD_STRING(isolate,
path)).FromMaybe(false);
```

NULL Pointer Dereference\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2838
Status New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	653
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
653.      suffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
suffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2839
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313 is not initialized when it is used by suffixArray at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 313.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	643	653
Object	0	suffixArray

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
643.    uint32_t index = 0;
....
653.      suffixArray->Set(context, index, TRI_V8_STD_STRING(isolate,
suffixes[s])).FromMaybe(false);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2840
Status	New

The variable declared in 0 at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 1291 is not initialized when it is used by Set at arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c in line 1291.

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	1372	1448
Object	0	Set

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method static void JS_RequestParts(v8::FunctionCallbackInfo<v8::Value> const& args) {

```
....
1372.         uint32_t j = 0;
....
1448.           result->Set(context, j++, partObject).FromMaybe(false);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2841
Status	New

The variable declared in 0 at arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	663	963
Object	0	_of

Code Snippet

File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c

Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.     return 0;
```

File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
963.       prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2842
Status	New

The variable declared in 0 at arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination

File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	663	961
Object	0	_of

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
961.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2843
Status	New

The variable declared in 0 at arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	663	963
Object	0	_of

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
963.      prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2844
Status	New

The variable declared in 0 at arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	663	961
Object	0	_of

Code Snippet

File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c

Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
961.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2845
Status	New

The variable declared in 0 at arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c

Line	663	963
Object	0	_of

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
963.      prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2846
Status	New

The variable declared in 0 at arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	663	961
Object	0	_of

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
961.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2847
Status	New

The variable declared in 0 at arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	663	963
Object	0	_of

Code Snippet

File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c

Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
963.      prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2848
Status	New

The variable declared in 0 at arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	663	961
Object	0	_of

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
961.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2849
Status	New

The variable declared in 0 at arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	663	963
Object	0	_of

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
963.      prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 48:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2850
Status	New

The variable declared in 0 at arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	663	961
Object	0	_of

Code Snippet

File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c

Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
961.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2851
Status	New

The variable declared in 0 at arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Line	663	963
Object	0	_of

Code Snippet

File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c

Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
963.      prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2852
Status	New

The variable declared in 0 at arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c in line 631 is not initialized when it is used by _of at arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c in line 830.

	Source	Destination
File	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Line	663	961
Object	0	_of

Code Snippet

File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c

Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
663.    return 0;
```

File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
961.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

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)

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2694
Status	New

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	buffer

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2695
Status	New

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	buffer

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2696
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	buffer

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2697
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	buffer

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2698
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-	arendst@@Tasmota-v12.4.0-CVE-2022-

	47021-TP.c	47021-TP.c
Line	152	152
Object	buffer	buffer

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2699
Status New

	Source	Destination
File	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	buffer

Code Snippet
File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2700
Status New

	Source	Destination
File	arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	buffer

Code Snippet

File Name	arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c
Method	static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2701
Status	New

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	buffer

Code Snippet

File Name	arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c
Method	static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2702
Status	New

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	buffer

Code Snippet

File Name	arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c
Method	static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2703
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Line	6386	6386
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2704
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Line	6388	6388
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2705
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Line	6386	6386
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2706
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Line	6388	6388
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2707
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Line	6386	6386

Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2708
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Line	6388	6388
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2709
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Line	6386	6386
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.          fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2710
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Line	6388	6388
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.          fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2711
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Line	6386	6386
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.          fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2712
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Line	6388	6388
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2713
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Line	6386	6386
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2714
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Line	6388	6388
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.10-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2715
Status New

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Line	6386	6386
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2716
Status New

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c	arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Line	6388	6388

Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2020-11080-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2717
Status New

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Line	6386	6386
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6386.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2718
Status New

	Source	Destination
File	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c	arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Line	6388	6388
Object	fprintf	fprintf

Code Snippet
File Name arangodb@@arangodb-v3.9.6-CVE-2024-28182-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6388.          fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2719
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	1037	1037
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1037.              fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2720
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Line	165	165
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.17.0-rc1-CVE-2023-31794-FP.c
Method infousage(void)

```
....
165.        fprintf(stderr,
```

Improper Resource Access Authorization\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2721
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	1037	1037
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1037.             fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2722
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Line	165	165
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.0-rc1-CVE-2023-31794-FP.c
Method infousage(void)

```
....
165.        fprintf(stderr,
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2723
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	1042	1042
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1042.             fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2724
Status New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Line	165	165
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.1-ios-CVE-2023-31794-FP.c
Method infousage(void)

```
....
165.        fprintf(stderr,
```

Improper Resource Access Authorization\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2725
Status New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	1042	1042

Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1042.             fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2726
Status New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Line	165	165
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.18.1-so-3.12.2b1-android-CVE-2023-31794-TP.c
Method infousage(void)

```
....
165.         fprintf(stderr,
```

Improper Resource Access Authorization\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2727
Status New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	1064	1064
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1064.             fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2728
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Line	187	187
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-appkit-2.1.0-CVE-2023-31794-TP.c
Method infousage(void)

```
....
187.         fprintf(stderr,
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2729
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	1064	1064
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1064.             fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2730
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Line	187	187
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.19.0-rc2-CVE-2023-31794-FP.c
Method infousage(void)

```
....
187.        fprintf(stderr,
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2731
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	1066	1066
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1066.            fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2732
Status	New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c	ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Line	187	187
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.20.0-rc2-CVE-2023-31794-TP.c
Method infousage(void)

```
....
187.        fprintf(stderr,
```

Improper Resource Access Authorization\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2733
Status New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	1054	1054
Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method int pdfinfo_main(int argc, char **argv)

```
....
1054.            fprintf(stderr, "cannot initialise context\n");
```

Improper Resource Access Authorization\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2734
Status New

	Source	Destination
File	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c	ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Line	187	187

Object	fprintf	fprintf

Code Snippet
File Name ArtifexSoftware@@mupdf-1.21.0-rc1-CVE-2023-31794-FP.c
Method infousage(void)

```
....
187.        fprintf(stderr,
```

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=1000007&projectid=1&pathid=2859
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	508	508
Object	ContentLength	ContentLength

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
508.        headers[StaticStrings::ContentLength] =
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2860
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c

Line	523	523
Object	ContentLength	ContentLength

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
523.        headers[StaticStrings::ContentLength] =
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2861
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	536	536
Object	ContentLength	ContentLength

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
536.        headers[StaticStrings::ContentLength] =
StringUtils::itoa(jsonString.size());
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2862
Status New

	Source	Destination
File	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c
Line	537	537
Object	ContentTypeHeader	ContentTypeHeader

Code Snippet
File Name arangodb@@arangodb-v3.8.0-alpha.1-CVE-2021-25939-FP.c

Method	v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
537.        headers[StaticStrings::ContentTypeHeader] =
StaticStrings::MimeTypeJson;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2863
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	508	508
Object	ContentLength	ContentLength

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
508.        headers[StaticStrings::ContentLength] =
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2864
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	523	523
Object	ContentLength	ContentLength

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
523.        headers[StaticStrings::ContentLength] =
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2865
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	536	536
Object	ContentLength	ContentLength

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
536.        headers[StaticStrings::ContentLength] =
StringUtils::itoa(jsonString.size());
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2866
Status	New

	Source	Destination
File	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c	arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Line	537	537
Object	ContentTypeHeader	ContentTypeHeader

Code Snippet
File Name arangodb@@arangodb-v3.8.3-preview.3-CVE-2021-25939-FP.c
Method v8::Handle<v8::Object> TRI_RequestCppToV8(v8::Isolate* isolate,

```
....
537.        headers[StaticStrings::ContentTypeHeader] =
StaticStrings::MimeTypeJson;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&

	pathid=2867
Status	New

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	154	154
Object	n	n

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
154.                m_URLSuffix[n] = '\0';
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2868
Status	New

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	159	159
Object	n	n

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
159.                m_URLPreSuffix[n] = '\0';
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2869
Status	New

	Source	Destination

File	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	154	154
Object	n	n

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
154.                m_URLSuffix[n] = '\0';
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2870
Status New

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	159	159
Object	n	n

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
159.                m_URLPreSuffix[n] = '\0';
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2871
Status New

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	154	154

Object	n	n

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
154.              m_URLSuffix[n] = '\0';
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2872
Status New

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	159	159
Object	n	n

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
159.              m_URLPreSuffix[n] = '\0';
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2873
Status New

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	154	154
Object	n	n

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c

Method	bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
154.            m_URLSuffix[n] = '\0';
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2874
Status	New

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	159	159
Object	n	n

Code Snippet	
File Name	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method	bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
159.            m_URLPreSuffix[n] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2875
Status	New

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	154	154
Object	n	n

Code Snippet	
File Name	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method	bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
154.                m_URLSuffix[n] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2876
Status	New

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	159	159
Object	n	n

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method bool CRtspSession::ParseRtspRequest(char const * aRequest, unsigned aRequestSize)

```
....
159.                m_URLPreSuffix[n] = '\0';
```

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=1000007&projectid=1&pathid=418
Status	New

The size of the buffer used by op_get_data in _nbytes, at line 147 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 147 of arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-	arendst@@Tasmota-v10.0.0-CVE-2022-

	47021-TP.c	47021-TP.c
Line	152	152
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=419
Status	New

The size of the buffer used by op_get_data in _nbytes, at line 147 of arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 147 of arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=420
Status	New

The size of the buffer used by op_get_data in _nbytes, at line 147 of arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 147 of arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination

File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=421
Status New

The size of the buffer used by op_get_data in _nbytes, at line 147 of arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 147 of arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=422
Status New

The size of the buffer used by op_get_data in _nbytes, at line 147 of arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 147 of arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=423
Status New

The size of the buffer used by op_get_data in _nbytes, at line 147 of arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 147 of arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Line	152	152
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
152.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=424
Status New

The size of the buffer used by op_get_data in _nbytes, at line 146 of arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that op_get_data passes to buffer, at line 146 of arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=425
Status New

The size of the buffer used by op_get_data in _nbytes, at line 146 of arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 146 of arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Heuristic 2nd Order Buffer Overflow read\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=426
Status New

The size of the buffer used by op_get_data in _nbytes, at line 146 of arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 146 of arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c, to overwrite the target buffer.

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c
Line	151	151
Object	buffer	_nbytes

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=427
Status New

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	735	735
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
735.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 2:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=428
Status	New

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	735	735
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
735.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=429
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	735	735
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
735.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=430
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	735	735
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
735.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=431
Status New

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	735	735
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
735.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=432
Status New

	Source	Destination
File	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Line	735	735

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
735.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=433
Status New

	Source	Destination
File	arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c
Line	734	734
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v9.1.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
734.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=434
Status New

	Source	Destination
File	arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c
Line	734	734
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
734.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

Arithmenic Operation On Boolean\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=435
Status	New

	Source	Destination
File	arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c
Line	734	734
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-47021-TP.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
734.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

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=1000007&projectid=1&pathid=2797
Status	New

	Source	Destination
File	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Line	1406	1425
Object	sr	sizeof

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
....
1425.    ret =
op_bisect_forward_serialno(_of,data_offset,sr,sizeof(sr)/sizeof(*sr),
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2798
Status	New

	Source	Destination
File	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Line	1406	1425
Object	sr	sizeof

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
....
1425.    ret =
op_bisect_forward_serialno(_of,data_offset,sr,sizeof(sr)/sizeof(*sr),
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2799
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Line	1406	1425
Object	sr	sizeof

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
....
1425.    ret =
op_bisect_forward_serialno(_of,data_offset,sr,sizeof(sr)/sizeof(*sr),
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2800
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Line	1406	1425
Object	sr	sizeof

Code Snippet
File Name arendst@@Tasmota-v12.2.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
....
1425.    ret =
op_bisect_forward_serialno(_of,data_offset,sr,sizeof(sr)/sizeof(*sr),
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2801
Status	New

	Source	Destination
File	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Line	1406	1425
Object	sr	sizeof

Code Snippet
File Name arendst@@Tasmota-v12.4.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
....
1425.    ret =
op_bisect_forward_serialno(_of,data_offset,sr,sizeof(sr)/sizeof(*sr),
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2802
Status	New

	Source	Destination
File	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c	arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Line	1406	1425
Object	sr	sizeof

Code Snippet
File Name arendst@@Tasmota-v13.0.0-CVE-2022-47021-TP.c
Method static int op_open_seekable2_impl(OggOpusFile *_of){

```
....
1406.    OpusSeekRecord *sr = (OpusSeekRecord*)malloc(64 *
sizeof(OpusSeekRecord));
....
1425.    ret =
op_bisect_forward_serialno(_of,data_offset,sr,sizeof(sr)/sizeof(*sr),
```

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=1000007&projectid=1&pathid=2735
Status	New

Method CRtspSession::Handle_RtspDESCRIBE at line 242 of arendst@@Tasmota-v10.0.0-CVE-2022-43294-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	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Line	278	278
Object	rand	rand

Code Snippet
File Name arendst@@Tasmota-v10.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
278.                rand(),
```

Use of Insufficiently Random Values\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2736
Status New

Method CRtspSession::Handle_RtspDESCRIBE at line 242 of arendst@@Tasmota-v11.0.0-CVE-2022-43294-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	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Line	278	278
Object	rand	rand

Code Snippet
File Name arendst@@Tasmota-v11.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
278.                rand(),
```

Use of Insufficiently Random Values\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2737
Status New

Method CRtspSession::Handle_RtspDESCRIBE at line 242 of arendst@@Tasmota-v12.0.0-CVE-2022-43294-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	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Line	278	278
Object	rand	rand

Code Snippet
File Name arendst@@Tasmota-v12.0.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
278.                rand(),
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2738
Status	New

Method CRtspSession::Handle_RtspDESCRIBE at line 242 of arendst@@Tasmota-v9.3.0-CVE-2022-43294-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	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Line	278	278
Object	rand	rand

Code Snippet
File Name arendst@@Tasmota-v9.3.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
278.                rand(),
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000007&projectid=1&pathid=2739
Status	New

Method CRtspSession::Handle_RtspDESCRIBE at line 242 of arendst@@Tasmota-v9.5.0-CVE-2022-43294-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	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c	arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Line	278	278
Object	rand	rand

Code Snippet
File Name arendst@@Tasmota-v9.5.0-CVE-2022-43294-TP.c
Method void CRtspSession::Handle_RtspDESCRIBE()

```
....
278.                rand(),
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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

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;
}
```

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;
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;
```

```
  void setPassword()
 {
      password = System.console().readLine("Enter your password: ");
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}
```

```
int main()
{
    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n'){
                  password[i]='\0';
                  break;
            } else{
                  password[i++]=ch;
                  fflush(0);
            }
      }
      i=0;
      memset(password,'\0',256);
}

int main()
{
      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n')
                  break;
      }
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of 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());
```

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

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Improper 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

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

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

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