vul_files_11 Scan Report

Project Name	vul_files_11
Scan Start	Monday, January 6, 2025 10:56:48 PM
Preset	Checkmarx Default
Scan Time	01h:06m:37s
Lines Of Code Scanned	299315
Files Scanned	172
Report Creation Time	Tuesday, January 7, 2025 10:16:29 AM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	7/1000 (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

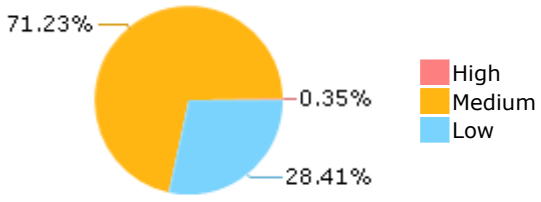
Results Limit

Results limit per query was set to 50

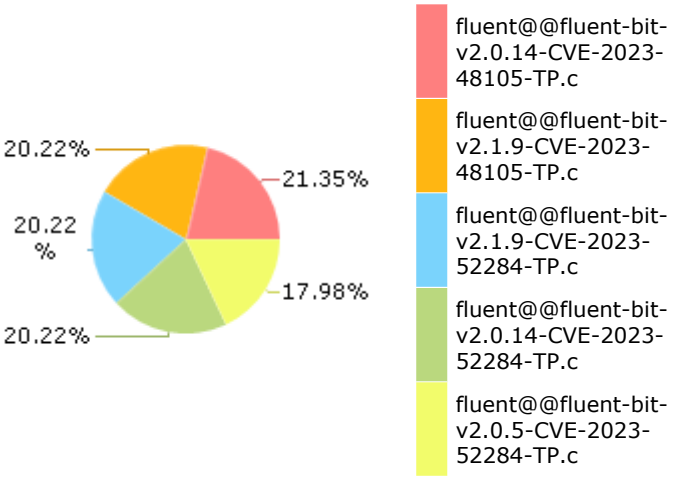
Selected Queries

Selected queries are listed in Result Summary

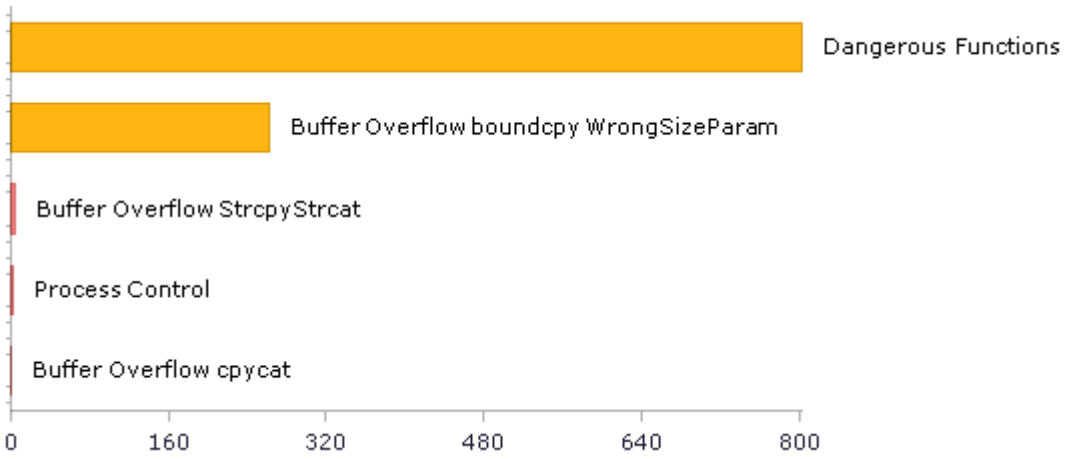
Result Summary



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	388	355
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	9	9
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	5	5
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	875	875
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	2	1
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	5	5
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	875	875
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	29	28
PCI DSS (3.2) - 6.5.2 - Buffer overflows	293	293
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	1	1
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	16	16
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.	12	12
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.	15	15
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.	5	5
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.	5	3

***** 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)	21	21
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)	7	7
SC-4 Information in Shared Resources (P1)	5	5
SC-5 Denial of Service Protection (P1)*	378	261
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	45	43
SI-11 Error Handling (P2)*	207	207
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	27	27

***** 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

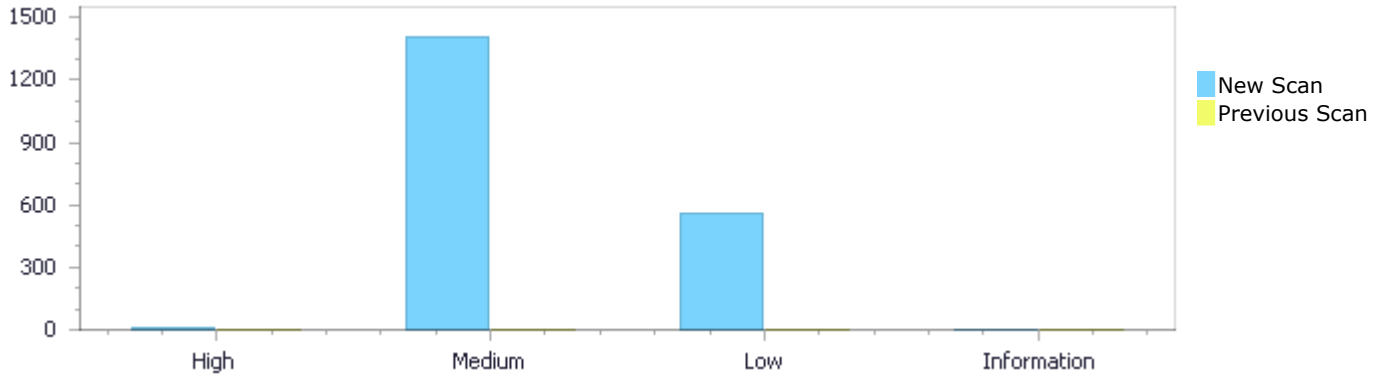
Scan Summary - Custom

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	7	1,409	562	0	1,978
Recurrent Issues	0	0	0	0	0
Total	7	1,409	562	0	1,978
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	7	1,409	562	0	1,978
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	7	1,409	562	0	1,978

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	4	High
Process Control	2	High
Buffer Overflow cpycat	1	High
Dangerous Functions	803	Medium
Buffer Overflow boundcpy WrongSizeParam	263	Medium

Use of Zero Initialized Pointer	199	Medium
Memory Leak	72	Medium
MemoryFree on StackVariable	30	Medium
Char Overflow	18	Medium
Buffer Overflow AddressOfLocalVarReturned	6	Medium
Heap Inspection	5	Medium
Use of Uninitialized Pointer	4	Medium
Divide By Zero	2	Medium
Download of Code Without Integrity Check	2	Medium
Stored Buffer Overflow fgets	2	Medium
Wrong Memory Allocation	2	Medium
Integer Overflow	1	Medium
Unchecked Return Value	207	Low
Use of Sizeof On a Pointer Type	97	Low
NULL Pointer Dereference	81	Low
Use of Obsolete Functions	72	Low
Potential Off by One Error in Loops	27	Low
Sizeof Pointer Argument	21	Low
Arithmenic Operation On Boolean	16	Low
Unchecked Array Index	13	Low
Exposure of System Data to Unauthorized Control Sphere	12	Low
Improper Resource Access Authorization	8	Low
Information Exposure Through Comments	7	Low
Incorrect Permission Assignment For Critical Resources	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c	40
fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c	40

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=1000023&projectid=13&pathid=2
Status	New

The size of the buffer used by main in ip_addr, at line 297 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 297 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	297	517
Object	argv	ip_addr

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
297.  main(int argc, char *argv[])
....
517.          strcpy(init_args.ip_addr, ip_addr);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=3
Status	New

The size of the buffer used by ntlm_current_time in timestamp, at line 181 of FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that ntlm_current_time passes to timestamp, at line 181 of FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c, to overwrite the target buffer.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	181	188
Object	timestamp	timestamp

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method void ntlm_current_time(BYTE* timestamp)

```
....
181.  void ntlm_current_time(BYTE* timestamp)
....
188.        CopyMemory(timestamp, &(time64.QuadPart), 8);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=4
Status New

The size of the buffer used by ntlm_generate_signing_key in exported_session_key, at line 594 of FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_generate_signing_key passes to exported_session_key, at line 594 of FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c, to overwrite the target buffer.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	594	606
Object	exported_session_key	exported_session_key

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method static int ntlm_generate_signing_key(BYTE* exported_session_key, PSecBuffer sign_magic,

```
....
594.  static int ntlm_generate_signing_key(BYTE* exported_session_key,
PSecBuffer sign_magic,
....
606.        CopyMemory(value, exported_session_key,
WINPR_MD5_DIGEST_LENGTH);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=5
Status	New

The size of the buffer used by ntlm_generate_sealing_key in exported_session_key, at line 655 of FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_generate_sealing_key passes to exported_session_key, at line 655 of FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c, to overwrite the target buffer.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	655	666
Object	exported_session_key	exported_session_key

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method static int ntlm_generate_sealing_key(BYTE* exported_session_key, PSecBuffer seal_magic,

```
....
655.  static int ntlm_generate_sealing_key(BYTE* exported_session_key,
PSecBuffer seal_magic,
....
666.        CopyMemory(p, exported_session_key,
WINPR_MD5_DIGEST_LENGTH);
```

Process Control

Query Path:
CPP\Cx\CPP High Risk\Process Control Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description
Process Control\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=6
Status	New

Method main at line 297 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c loads a library whose name or location is influenced by input from the client in the argv element. This element's value then flows through the code without being properly validated, in load_and_register_native_libs at line 203 of fluent@@fluent-bit-

v2.0.14-CVE-2023-48105-TP.c. Executing commands or loading libraries from an untrusted source or in an untrusted environment can cause an application to execute malicious commands.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	297	214
Object	argv	dlopen

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
297.  main(int argc, char *argv[])
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method load_and_register_native_libs(const char **native_lib_list,

```
....
214.          if (!(handle = dlopen(native_lib_list[i], RTLD_NOW |
RTLD_GLOBAL))
```

Process Control\Path 2:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=7
Status New

Method main at line 297 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c loads a library whose name or location is influenced by input from the client in the argv element. This element's value then flows through the code without being properly validated, in load_and_register_native_libs at line 203 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c. Executing commands or loading libraries from an untrusted source or in an untrusted environment can cause an application to execute malicious commands.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	297	215
Object	argv	dlopen

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
297.  main(int argc, char *argv[])
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c

Method load_and_register_native_libs(const char **native_lib_list,

```
....
215.              && !(handle = dlopen(native_lib_list[i], RTLD_LAZY)))
{
```

Buffer Overflow cpycat

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow cpycat 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

Buffer Overflow cpycat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1
Status	New

The size of the buffer used by main in ip_addr, at line 297 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 297 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	297	517
Object	argv	ip_addr

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
297.  main(int argc, char *argv[])
....
517.          strcpy(init_args.ip_addr, ip_addr);
```

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=1000023&projectid=13&pathid=328
Status	New

The dangerous function, CopyMemory, was found in use at line 994 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Line	997	997
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Method static BOOL update_set_bounds(rdpContext* context, const rdpBounds* bounds)

```
....
997.         CopyMemory(&update->previousBounds, &update->currentBounds,
sizeof(rdpBounds));
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=329
Status	New

The dangerous function, CopyMemory, was found in use at line 994 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Line	1002	1002
Object	CopyMemory	CopyMemory

Code Snippet	
File Name	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Method	static BOOL update_set_bounds(rdpContext* context, const rdpBounds* bounds)

```
....
1002.              CopyMemory(&update->currentBounds, bounds,
sizeof(rdpBounds));
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=330
Status	New

The dangerous function, CopyMemory, was found in use at line 395 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c
Line	469	469
Object	CopyMemory	CopyMemory

Code Snippet	
File Name	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c
Method	UINT cliprdr_read_format_list(wStream* s, CLIPRDR_FORMAT_LIST* formatList, BOOL useLongFormatNames)

```
....
469.
      CopyMemory(formats[index].formatName, szFormatName, 32);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=331
Status	New

The dangerous function, CopyMemory, was found in use at line 181 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-	FreeRDP@@FreeRDP-2.0.0-CVE-2020-

	11086-TP.c	11086-TP.c
Line	188	188
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method void ntlm_current_time(BYTE* timestamp)

```
....
188.        CopyMemory(timestamp, &(time64.QuadPart), 8);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=332
Status	New

The dangerous function, CopyMemory, was found in use at line 196 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	199	199
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method void ntlm_generate_timestamp(NTLM_CONTEXT* context)

```
....
199.              CopyMemory(context->Timestamp, context-
>ChallengeTimestamp, 8);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=333
Status	New

The dangerous function, CopyMemory, was found in use at line 372 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	392	392
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_lm_v2_response(NTLM_CONTEXT* context)

```
....
392.        CopyMemory(value, context->ServerChallenge, 8);
```

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=334
Status New

The dangerous function, CopyMemory, was found in use at line 372 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	393	393
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_lm_v2_response(NTLM_CONTEXT* context)

```
....
393.        CopyMemory(&value[8], context->ClientChallenge, 8);
```

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=335
Status New

The dangerous function, CopyMemory, was found in use at line 372 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	404	404
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_lm_v2_response(NTLM_CONTEXT* context)

```
....
404.        CopyMemory(&response[16], context->ClientChallenge, 8);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=336
Status	New

The dangerous function, CopyMemory, was found in use at line 415 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	439	439
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_ntlm_v2_response(NTLM_CONTEXT* context)

```
....
439.        CopyMemory(&blob[8], context->Timestamp, 8);        /*
Timestamp (8 bytes) */
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=337
Status	New

The dangerous function, CopyMemory, was found in use at line 415 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	440	440
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_ntlm_v2_response(NTLM_CONTEXT* context)

```
....
440.        CopyMemory(&blob[16], context->ClientChallenge, 8); /*
ClientChallenge (8 bytes) */
```

Dangerous Functions\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=338
Status New

The dangerous function, CopyMemory, was found in use at line 415 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	442	442
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_ntlm_v2_response(NTLM_CONTEXT* context)

```
....
442.        CopyMemory(&blob[28], TargetInfo->pvBuffer, TargetInfo-
>cbBuffer);
```

Dangerous Functions\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=339
Status	New

The dangerous function, CopyMemory, was found in use at line 415 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	454	454
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_ntlm_v2_response(NTLM_CONTEXT* context)

```
....
454.        CopyMemory(blob, context->ServerChallenge, 8);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=340
Status	New

The dangerous function, CopyMemory, was found in use at line 415 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	455	455
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_ntlm_v2_response(NTLM_CONTEXT* context)

```
....
455.        CopyMemory(&blob[8], ntlm_v2_temp.pvBuffer,
ntlm_v2_temp.cbBuffer);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=341
Status	New

The dangerous function, CopyMemory, was found in use at line 415 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	466	466
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_ntlm_v2_response(NTLM_CONTEXT* context)

```
....
466.        CopyMemory(blob, nt_proof_str, 16);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=342
Status	New

The dangerous function, CopyMemory, was found in use at line 415 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	467	467
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method int ntlm_compute_ntlm_v2_response(NTLM_CONTEXT* context)

```
....
467.        CopyMemory(&blob[16], ntlm_v2_temp.pvBuffer,
ntlm_v2_temp.cbBuffer);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=343
Status	New

The dangerous function, CopyMemory, was found in use at line 525 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	528	528
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method void ntlm_generate_key_exchange_key(NTLM_CONTEXT* context)

```
....
528.        CopyMemory(context->KeyExchangeKey, context->SessionBaseKey,
16);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=344
Status	New

The dangerous function, CopyMemory, was found in use at line 546 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	548	548
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method void ntlm_generate_exported_session_key(NTLM_CONTEXT* context)

```
....
548.        CopyMemory(context->ExportedSessionKey, context-
>RandomSessionKey, 16);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=345
Status	New

The dangerous function, CopyMemory, was found in use at line 569 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	583	583
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method void ntlm_decrypt_random_session_key(NTLM_CONTEXT* context)

```
....
583.             CopyMemory(context->RandomSessionKey, context-
>KeyExchangeKey, 16);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=346
Status	New

The dangerous function, CopyMemory, was found in use at line 594 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	606	606
Object	CopyMemory	CopyMemory

Code Snippet	
File Name	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method	static int ntlm_generate_signing_key(BYTE* exported_session_key, PSecBuffer sign_magic,

```
....
606.        CopyMemory(value, exported_session_key,
WINPR_MD5_DIGEST_LENGTH);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=347
Status	New

The dangerous function, CopyMemory, was found in use at line 594 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	607	607
Object	CopyMemory	CopyMemory

Code Snippet	
File Name	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method	static int ntlm_generate_signing_key(BYTE* exported_session_key, PSecBuffer sign_magic,

```
....
607.        CopyMemory(&value[WINPR_MD5_DIGEST_LENGTH], sign_magic-
>pvBuffer, sign_magic->cbBuffer);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=348
Status	New

The dangerous function, CopyMemory, was found in use at line 655 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-	FreeRDP@@FreeRDP-2.0.0-CVE-2020-

	11086-TP.c	11086-TP.c
Line	666	666
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method static int ntlm_generate_sealing_key(BYTE* exported_session_key, PSecBuffer seal_magic,

```
....
666.         CopyMemory(p, exported_session_key,
WINPR_MD5_DIGEST_LENGTH);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=349
Status	New

The dangerous function, CopyMemory, was found in use at line 655 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	667	667
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method static int ntlm_generate_sealing_key(BYTE* exported_session_key, PSecBuffer seal_magic,

```
....
667.         CopyMemory(&p[WINPR_MD5_DIGEST_LENGTH], seal_magic-
>pvBuffer, seal_magic->cbBuffer);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=350
Status	New

The dangerous function, CopyMemory, was found in use at line 1126 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	1167	1167
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_server_AuthenticateComplete(NTLM_CONTEXT* context)

```
....
1167.             CopyMemory(
```

Dangerous Functions\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=351
Status New

The dangerous function, CopyMemory, was found in use at line 112 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	114	114
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method static void ntlm_populate_message_header(NTLM_MESSAGE_HEADER* header, UINT32 MessageType)

```
....
114.         CopyMemory(header->Signature, NTLM_SIGNATURE,
sizeof(NTLM_SIGNATURE));
```

Dangerous Functions\Path 25:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=352
Status	New

The dangerous function, CopyMemory, was found in use at line 198 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	268	268
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_NegotiateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
268.         CopyMemory(context->NegotiateMessage.pvBuffer, buffer->pvBuffer, buffer->cbBuffer);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=353
Status	New

The dangerous function, CopyMemory, was found in use at line 285 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	348	348
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_write_NegotiateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
348.         CopyMemory(context->NegotiateMessage.pvBuffer, buffer->pvBuffer, buffer->cbBuffer);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=354
Status	New

The dangerous function, CopyMemory, was found in use at line 363 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	415	415
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_ChallengeMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
415.        CopyMemory(context->ServerChallenge, message->ServerChallenge, 8);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=355
Status	New

The dangerous function, CopyMemory, was found in use at line 363 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	477	477
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_ChallengeMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
477.                    CopyMemory(context->ChallengeTimestamp, ptr, 8);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=356
Status	New

The dangerous function, CopyMemory, was found in use at line 363 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	489	489
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_ChallengeMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
489.        CopyMemory(context->ChallengeMessage.pvBuffer, StartOffset,
length);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=357
Status	New

The dangerous function, CopyMemory, was found in use at line 581 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	604	604
Object	CopyMemory	CopyMemory

Code Snippet	
File Name	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method	SECURITY_STATUS ntlm_write_ChallengeMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
604.        CopyMemory(message->ServerChallenge, context-
>ServerChallenge, 8); /* ServerChallenge */
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=358
Status	New

The dangerous function, CopyMemory, was found in use at line 581 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	659	659
Object	CopyMemory	CopyMemory

Code Snippet	
File Name	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method	SECURITY_STATUS ntlm_write_ChallengeMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
659.        CopyMemory(context->ChallengeMessage.pvBuffer,
Stream_Buffer(s), length);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=359
Status	New

The dangerous function, CopyMemory, was found in use at line 677 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-	FreeRDP@@FreeRDP-2.0.0-CVE-2020-

	11087-TP.c	11087-TP.c
Line	825	825
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_AuthenticateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
825.              CopyMemory(context->ClientChallenge, context-
>NTLMv2Response.Challenge.ClientChallenge, 8);
```

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=360
Status New

The dangerous function, CopyMemory, was found in use at line 677 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	849	849
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_AuthenticateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
849.              CopyMemory(context->EncryptedRandomSessionKey,
message->EncryptedRandomSessionKey.Buffer,
```

Dangerous Functions\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=361
Status New

The dangerous function, CopyMemory, was found in use at line 677 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	861	861
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_AuthenticateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
861.        CopyMemory(context->AuthenticateMessage.pvBuffer,
Stream_Buffer(s), length);
```

Dangerous Functions\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=362
Status New

The dangerous function, CopyMemory, was found in use at line 677 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	914	914
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_AuthenticateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
914.              CopyMemory(credentials->identity.User, message-
>UserName.Buffer, message->UserName.Len);
```

Dangerous Functions\Path 36:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=363
Status	New

The dangerous function, CopyMemory, was found in use at line 677 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	928	928
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_read_AuthenticateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
928.              CopyMemory(credentials->identity.Domain, message->DomainName.Buffer,
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=364
Status	New

The dangerous function, CopyMemory, was found in use at line 946 in FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Line	1079	1079
Object	CopyMemory	CopyMemory

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11087-TP.c
Method SECURITY_STATUS ntlm_write_AuthenticateMessage(NTLM_CONTEXT* context, PSecBuffer buffer)

```
....
1079.       CopyMemory(context->AuthenticateMessage.pvBuffer,
Stream_Buffer(s), length);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=365
Status	New

The dangerous function, memcpy, was found in use at line 1243 in flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c
Line	1288	1288
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c
Method void subghz_on_system_start(void) {

```
....
1288.           memcpy(
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=366
Status	New

The dangerous function, memcpy, was found in use at line 1243 in flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c
Line	1288	1288
Object	memcpy	memcpy

Code Snippet

File Name	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c
Method	void subghz_on_system_start(void) {

```
....
1288.           memcpy(
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=367
Status	New

The dangerous function, memcpy, was found in use at line 1243 in flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c
Line	1288	1288
Object	memcpy	memcpy

Code Snippet

File Name	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c
Method	void subghz_on_system_start(void) {

```
....
1288.           memcpy(
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=368
Status	New

The dangerous function, memcpy, was found in use at line 164 in flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	233	233
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
233.          memcpy(sd_info->oem_id, info.oem_id, sizeof(info.oem_id));
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=369
Status	New

The dangerous function, memcpy, was found in use at line 164 in flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	234	234
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
234.          memcpy(sd_info->product_name, info.product_name,
sizeof(info.product_name));
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=370
Status	New

The dangerous function, memcpy, was found in use at line 457 in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Line	483	483

Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Method static bool nfc_device_save_mifare_df_data(FlipperFormat* file, NfcDevice* dev)
{

```
....
483.                memcpy(tmp + i, app->id, 3);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=371
Status	New

The dangerous function, memcpy, was found in use at line 497 in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Line	532	532
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Method bool nfc_device_load_mifare_df_data(FlipperFormat* file, NfcDevice* dev) {

```
....
532.                memcpy(app->id, &tmp[i * 3], 3);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=372
Status	New

The dangerous function, memcpy, was found in use at line 487 in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-	flipperdevices@@flipperzero-firmware-

	0.62.0-rc-CVE-2022-40363-TP.c	0.62.0-rc-CVE-2022-40363-TP.c
Line	514	514
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Method static bool nfc_device_save_mifare_df_data(FlipperFormat* file, NfcDevice* dev)
{

```
....
514.                    memcpy(tmp + i, app->id, 3);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=373
Status	New

The dangerous function, memcpy, was found in use at line 529 in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Line	567	567
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Method bool nfc_device_load_mifare_df_data(FlipperFormat* file, NfcDevice* dev) {

```
....
567.                    memcpy(app->id, &tmp[i * 3], 3);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=374
Status	New

The dangerous function, memcpy, was found in use at line 805 in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24805-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24805-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24805-FP.c
Line	850	850
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24805-FP.c
Method void subghz_on_system_start() {

```
....
850.            memcpy(
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=375
Status	New

The dangerous function, memcpy, was found in use at line 805 in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24807-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24807-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24807-FP.c
Line	850	850
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24807-FP.c
Method void subghz_on_system_start() {

```
....
850.            memcpy(
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=376
Status	New

The dangerous function, memcpy, was found in use at line 805 in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24808-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24808-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24808-FP.c
Line	850	850
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-24808-FP.c
Method void subghz_on_system_start() {

```
....
850.            memcpy(
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=377
Status	New

The dangerous function, memcpy, was found in use at line 810 in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-24805-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-24805-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-24805-FP.c
Line	855	855
Object	memcpy	memcpy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-24805-FP.c
Method void subghz_on_system_start() {

```
....
855.            memcpy(
```

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=1000023&projectid=13&pathid=14
Status	New

The size of the buffer used by sd_card_info in Namespace988367865, at line 164 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace988367865, at line 164 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	233	233
Object	Namespace988367865	Namespace988367865

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
233.          memcpy(sd_info->oem_id, info.oem_id, sizeof(info.oem_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=15
Status	New

The size of the buffer used by sd_card_info in Namespace988367865, at line 164 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace988367865, at line 164 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	234	234
Object	Namespace988367865	Namespace988367865

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
234.          memcpy(sd_info->product_name, info.product_name,
sizeof(info.product_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=16
Status	New

The size of the buffer used by picopass_read_preauth in Namespace1018191440, at line 114 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_preauth passes to Namespace1018191440, at line 114 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	132	132
Object	Namespace1018191440	Namespace1018191440

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_read_preauth(PicopassBlock* AA1) {

```
....
132.      memcpy(AA1[PICOPASS_CSN_BLOCK_INDEX].data, selRes.CSN,
sizeof(selRes.CSN));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=17
Status	New

The size of the buffer used by picopass_read_preauth in Namespace1018191440, at line 114 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_preauth passes to Namespace1018191440, at line 114 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	147	147

Object	Namespace1018191440	Namespace1018191440

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_read_preauth(PicopassBlock* AA1) {

```
....
147.      memcpy(AA1[PICOPASS_CONFIG_BLOCK_INDEX].data, cfg.data,
sizeof(cfg.data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=18
Status	New

The size of the buffer used by picopass_read_preauth in Namespace1018191440, at line 114 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_preauth passes to Namespace1018191440, at line 114 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	162	162
Object	Namespace1018191440	Namespace1018191440

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_read_preauth(PicopassBlock* AA1) {

```
....
162.      memcpy(AA1[PICOPASS_AIA_BLOCK_INDEX].data, aia.data,
sizeof(aia.data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=19
Status	New

The size of the buffer used by picopass_auth_standard in Namespace1018191440, at line 178 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_auth_standard passes to Namespace1018191440, at line 178 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	192	192
Object	Namespace1018191440	Namespace1018191440

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method static ReturnCode picopass_auth_standard(uint8_t* csn, uint8_t* div_key) {

```
....
192.      memcpy(ccnr, rcRes.CCNR, sizeof(rcRes.CCNR)); // last 4 bytes
left 0
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=20
Status	New

The size of the buffer used by picopass_auth_dict in Namespace1018191440, at line 200 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_auth_dict passes to Namespace1018191440, at line 200 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	247	247
Object	Namespace1018191440	Namespace1018191440

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method static ReturnCode picopass_auth_dict(

```
....
247.          memcpy(ccnr, rcRes.CCNR, sizeof(rcRes.CCNR)); // last 4
bytes left 0
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=21
Status	New

The size of the buffer used by picopass_read_card in Namespace1018191440, at line 297 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_card passes to Namespace1018191440, at line 297 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	330	330
Object	Namespace1018191440	Namespace1018191440

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_read_card(PicopassBlock* AA1) {

```
....
330.          memcpy(AA1[i].data, block.data, sizeof(block.data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=22
Status New

The size of the buffer used by picopass_write_card in Namespace1018191440, at line 336 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_write_card passes to Namespace1018191440, at line 336 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	365	365
Object	Namespace1018191440	Namespace1018191440

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_write_card(PicopassBlock* AA1) {

```
....
365.      memcpy(ccnr, rcRes.CCNR, sizeof(rcRes.CCNR)); // last 4 bytes
left 0
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=23
Status	New

The size of the buffer used by picopass_read_preauth in Namespace1010369364, at line 109 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_preauth passes to Namespace1010369364, at line 109 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	127	127
Object	Namespace1010369364	Namespace1010369364

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_read_preauth(PicopassBlock* AA1) {

```
....
127.      memcpy(AA1[PICOPASS_CSN_BLOCK_INDEX].data, selRes.CSN,
sizeof(selRes.CSN));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=24
Status	New

The size of the buffer used by picopass_read_preauth in Namespace1010369364, at line 109 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_preauth passes to Namespace1010369364, at line 109 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	142	142
Object	Namespace1010369364	Namespace1010369364

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_read_preauth(PicopassBlock* AA1) {

```
....
142.      memcpy(AA1[PICOPASS_CONFIG_BLOCK_INDEX].data, cfg.data,
sizeof(cfg.data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=25
Status	New

The size of the buffer used by picopass_read_preauth in Namespace1010369364, at line 109 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_preauth passes to Namespace1010369364, at line 109 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	157	157
Object	Namespace1010369364	Namespace1010369364

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_read_preauth(PicopassBlock* AA1) {

```
....
157.      memcpy(AA1[PICOPASS_AIA_BLOCK_INDEX].data, aia.data,
sizeof(aia.data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=26
Status	New

The size of the buffer used by picopass_auth_dict in Namespace1010369364, at line 174 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_auth_dict passes to Namespace1010369364, at line 174 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	226	226
Object	Namespace1010369364	Namespace1010369364

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c

Method	picopass_auth_dict(PicopassWorker* picopass_worker, IclassEliteDictType dict_type) {

```
....
226.          memcpy(ccnr, rcRes.CCNR, sizeof(rcRes.CCNR)); // last 4
bytes left 0
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=27
Status	New

The size of the buffer used by picopass_read_card in Namespace1010369364, at line 269 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_read_card passes to Namespace1010369364, at line 269 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	302	302
Object	Namespace1010369364	Namespace1010369364

Code Snippet

File Name	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method	ReturnCode picopass_read_card(PicopassBlock* AA1) {

```
....
302.          memcpy(AA1[i].data, block.data, sizeof(block.data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=28
Status	New

The size of the buffer used by picopass_write_card in Namespace1010369364, at line 308 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_write_card passes to Namespace1010369364, at line 308 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	337	337

Object	Namespace1010369364	Namespace1010369364

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_write_card(PicopassBlock* AA1) {

```
....
337.      memcpy(ccnr, rcRes.CCNR, sizeof(rcRes.CCNR)); // last 4 bytes
left 0
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=29
Status	New

The size of the buffer used by picopass_write_block in Namespace1010369364, at line 381 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_write_block passes to Namespace1010369364, at line 381 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	409	409
Object	Namespace1010369364	Namespace1010369364

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_write_block(PicopassBlock* AA1, uint8_t blockNo, uint8_t* newBlock) {

```
....
409.      memcpy(ccnr, rcRes.CCNR, sizeof(rcRes.CCNR)); // last 4 bytes
left 0
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=30
Status	New

The size of the buffer used by picopass_worker_elite_dict_attack in Namespace1010369364, at line 461 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that picopass_worker_elite_dict_attack passes to Namespace1010369364, at line 461 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	541	541
Object	Namespace1010369364	Namespace1010369364

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method void picopass_worker_elite_dict_attack(PicopassWorker* picopass_worker) {

```
....
541.          memcpy(ccnr, rcRes.CCNR, sizeof(rcRes.CCNR)); // last 4
bytes left 0
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=31
Status New

The size of the buffer used by sd_card_info in Namespace1317756588, at line 138 of flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace1317756588, at line 138 of flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Line	207	207
Object	Namespace1317756588	Namespace1317756588

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
207.          memcpy(sd_info->oem_id, cid.OEM_AppliID,
sizeof(cid.OEM_AppliID));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=32
Status New

The size of the buffer used by sd_card_info in Namespace1317756588, at line 138 of flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace1317756588, at line 138 of flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Line	208	208
Object	Namespace1317756588	Namespace1317756588

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
208.          memcpy(sd_info->product_name, cid.ProdName,
sizeof(cid.ProdName));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=33
Status New

The size of the buffer used by sd_card_info in Namespace1660936329, at line 164 of flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace1660936329, at line 164 of flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	233	233
Object	Namespace1660936329	Namespace1660936329

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
233.          memcpy(sd_info->oem_id, info.oem_id, sizeof(info.oem_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=34
Status	New

The size of the buffer used by sd_card_info in Namespace1660936329, at line 164 of flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace1660936329, at line 164 of flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	234	234
Object	Namespace1660936329	Namespace1660936329

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
234.          memcpy(sd_info->product_name, info.product_name,
sizeof(info.product_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=35
Status	New

The size of the buffer used by sd_card_info in Namespace1193205995, at line 164 of flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace1193205995, at line 164 of flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	233	233
Object	Namespace1193205995	Namespace1193205995

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
233.          memcpy(sd_info->oem_id, info.oem_id, sizeof(info.oem_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=36
Status	New

The size of the buffer used by sd_card_info in Namespace1193205995, at line 164 of flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to Namespace1193205995, at line 164 of flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	234	234
Object	Namespace1193205995	Namespace1193205995

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
234.          memcpy(sd_info->product_name, info.product_name,
sizeof(info.product_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=37
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Line	2977	2977
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2977.                          memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=38
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Line	2980	2980
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2980.                          memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=39
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Line	2977	2977
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet	
File Name	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Method	message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2977.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=40
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Line	2980	2980
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet	
File Name	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Method	message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2980.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=41
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c

Line	2977	2977
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2977.                          memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=42
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Line	2980	2980
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2980.                          memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=43
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Line	2977	2977
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2977.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=44
Status New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Line	2980	2980
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2980.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=45
Status New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Line	2977	2977
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2977.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=46
Status New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Line	2980	2980
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2980.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=47
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Line	2979	2979
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2979.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=48
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Line	2982	2982
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2982.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=49
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Line	2979	2979
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2979.                          memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=50
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Line	2982	2982
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2982.                          memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=51
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Line	2979	2979
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2979.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=52
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Line	2982	2982
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2982.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=53
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Line	2979	2979
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2979.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=54
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Line	2982	2982
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet	
File Name	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Method	message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2982.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=55
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2945 of fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Line	2979	2979
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet	
File Name	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Method	message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2979.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=56
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2945 of fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Line	2982	2982

Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2982.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=57
Status	New

The size of the buffer used by session_new in session_ptr, at line 434 of fluent@@fluent-bit-v3.0.1-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 434 of fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c
Line	533	533
Object	session_ptr	session_ptr

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c
Method static int session_new(nghttp2_session **session_ptr,

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

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=58
Status	New

The size of the buffer used by session_new in session_ptr, at line 434 of fluent@@fluent-bit-v3.0.1-CVE-2024-4323-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 434 of fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-	fluent@@fluent-bit-v3.0.1-CVE-2024-

	4323-TP.c	4323-TP.c
Line	533	533
Object	session_ptr	session_ptr

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c
Method static int session_new(nghttp2_session **session_ptr,

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

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=59
Status New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2943 of fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Line	2977	2977
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2977.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=60
Status New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2943 of fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Line	2980	2980
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2980.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=61
Status	New

The size of the buffer used by map_eapsim_basictypes in total_length, at line 63 of FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that map_eapsim_basictypes passes to total_length, at line 63 of FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c, to overwrite the target buffer.

	Source	Destination
File	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c
Line	244	244
Object	total_length	total_length

Code Snippet
File Name FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c
Method int map_eapsim_basictypes(RADIUS_PACKET *r, eap_packet_t *ep)

```
....
244.              memcpy(hdr->length, &total_length,
sizeof(total_length));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=62
Status	New

The size of the buffer used by sd_card_info in SDInfo, at line 164 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sd_card_info passes to SDInfo, at line 164 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	173	173
Object	SDInfo	SDInfo

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method FS_Error sd_card_info(StorageData* storage, SDInfo* sd_info) {

```
....
173.      memset(sd_info, 0, sizeof(SDInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=63
Status New

The size of the buffer used by fs_file_open in SDFileDirStorage, at line 195 of flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fs_file_open passes to SDFileDirStorage, at line 195 of flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-3520-FP.c
Line	205	205
Object	SDFileDirStorage	SDFileDirStorage

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-3520-FP.c
Method bool fs_file_open(File* file, const char* path, FS_AccessMode access_mode, FS_OpenMode open_mode) {

```
....
205.              memset(&(filedata->data), 0,
sizeof(SDFileDirStorage));
```

Use of Zero Initialized Pointer

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

Categories

Description

Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1214
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c in line 339 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c in line 339.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Line	341	482
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
341.      void* pvReturn = NULL;
....
482.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1215
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-32020-FP.c in line 212 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-32020-FP.c in line 212.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-32020-FP.c
Line	214	330
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.20.0-CVE-2021-32020-FP.c

Method	void* pvPortMalloc(size_t xWantedSize) {

```
....
214.      void* pvReturn = NULL;
....
330.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1216
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.3.0-CVE-2021-32020-FP.c in line 97 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.3.0-CVE-2021-32020-FP.c in line 97.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.3.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.3.0-CVE-2021-32020-FP.c
Line	99	214
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.3.0-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
99.       void* pvReturn = NULL;
....
214.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1217
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-32020-FP.c in line 240 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-32020-FP.c in line 240.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-32020-FP.c

Line	242	358
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
242.      void* pvReturn = NULL;
....
358.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1218
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-32020-FP.c in line 240 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-32020-FP.c in line 240.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-32020-FP.c
Line	242	358
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
242.      void* pvReturn = NULL;
....
358.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1219
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c in line 329 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c in line 329.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Line	331	468
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
331.      void* pvReturn = NULL;
....
468.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1220
Status New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c in line 339 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c in line 339.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Line	341	478
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
341.      void* pvReturn = NULL;
....
478.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1221
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c in line 338 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c in line 338.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c
Line	340	477
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
340.      void* pvReturn = NULL;
....
477.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1222
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c in line 339 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c in line 339.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Line	341	482
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
341.      void* pvReturn = NULL;
....
482.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1223
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c in line 339 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c in line 339.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Line	341	482
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
341.      void* pvReturn = NULL;
....
482.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1224
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c in line 339 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c in line 339.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Line	341	482

Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
341.      void* pvReturn = NULL;
....
482.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1225
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c in line 340 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c in line 340.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Line	342	483
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
342.      void* pvReturn = NULL;
....
483.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1226
Status	New

The variable declared in pvReturn at flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c in line 344 is not initialized when it is used by pvReturn at flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c in line 344.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Line	346	487
Object	pvReturn	pvReturn

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Method void* pvPortMalloc(size_t xWantedSize) {

```
....
346.      void* pvReturn = NULL;
....
487.      configASSERT((((size_t)pvReturn) &
(size_t)portBYTE_ALIGNMENT_MASK) == 0);
```

Use of Zero Initialized Pointer\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1227
Status New

The variable declared in res at fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c in line 109 is not initialized when it is used by res at fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c in line 109.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	111	120
Object	res	res

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method split_string(char *str, int *count)

```
....
111.      char **res = NULL, **res1;
....
120.          res = (char **)realloc(res1, sizeof(char *) * (uint32)(idx
+ 1));
```

Use of Zero Initialized Pointer\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1228
Status New

The variable declared in linked_attachment at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 453 is not initialized when it is used by linked_func at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 453.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	464	475
Object	linked_attachment	linked_func

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
464.      void *linked_attachment = NULL;
....
475.      linked_func = wasm_native_resolve_symbol(
```

Use of Zero Initialized Pointer\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1229
Status New

The variable declared in linked_signature at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 453 is not initialized when it is used by linked_func at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 453.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	463	475
Object	linked_signature	linked_func

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
463.      const char *linked_signature = NULL;
....
475.      linked_func = wasm_native_resolve_symbol(
```

Use of Zero Initialized Pointer\Path 17:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1230
Status	New

The variable declared in import_functions at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693 is not initialized when it is used by import_functions at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	701	824
Object	import_functions	import_functions

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
701.      WASMImport *import_functions = NULL, *import_tables = NULL;
....
824.                        import = import_functions++;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1231
Status	New

The variable declared in import_memories at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693 is not initialized when it is used by import_memories at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	702	846
Object	import_memories	import_memories

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
702.      WASMImport *import_memories = NULL, *import_globals = NULL;
....
846.                          import = import_memories++;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1232
Status	New

The variable declared in sub_module at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693 is not initialized when it is used by sub_module at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	793	872
Object	sub_module	sub_module

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
793.              WASMModule *sub_module = NULL;
....
872.              (void)sub_module;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1233
Status	New

The variable declared in types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3877 is not initialized when it is used by types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3877.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	3892	3915
Object	types	types

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	wasm_loader_emit_br_info(WASMLoaderContext *ctx, BranchBlock *frame_csp,

```
....
3892.       uint8 *types = NULL, cell;
....
3915.               cell = (uint8)wasm_value_type_cell_num(types[i]);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1234
Status	New

The variable declared in types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3877 is not initialized when it is used by types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3877.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	3892	3920
Object	types	types

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	wasm_loader_emit_br_info(WASMLoaderContext *ctx, BranchBlock *frame_csp,

```
....
3892.       uint8 *types = NULL, cell;
....
3920.               cell = (uint8)wasm_value_type_cell_num(types[i]);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1235
Status	New

The variable declared in types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3877 is not initialized when it is used by types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3877.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	3892	3928

Object	types	types

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_emit_br_info(WASMLoaderContext *ctx, BranchBlock *frame_csp,

```
....
3892.      uint8 *types = NULL, cell;
....
3928.              cell = (uint8)wasm_value_type_cell_num(types[i]);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1236
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419 is not initialized when it is used by return_types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4426	4437
Object	return_types	return_types

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4426.      uint8 *return_types = NULL;
....
4437.          uint8 cell =
(uint8)wasm_value_type_cell_num(return_types[0]);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1237
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419 is not initialized when it is used by return_types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419.

	Source	Destination

File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4426	4477
Object	return_types	return_types

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4426.      uint8 *return_types = NULL;
....
4477.          uint8 cells =
(uint8)wasm_value_type_cell_num(return_types[i]);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1238
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419 is not initialized when it is used by return_types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4426	4518
Object	return_types	return_types

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4426.      uint8 *return_types = NULL;
....
4518.              uint8 cell =
(uint8)wasm_value_type_cell_num(return_types[i]);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1239
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419 is not initialized when it is used by dst_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4426	4527
Object	return_types	dst_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4426.      uint8 *return_types = NULL;
....
4527.                  dst_offsets[j] = dynamic_offset;
```

Use of Zero Initialized Pointer\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1240
Status New

The variable declared in src_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419 is not initialized when it is used by src_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4490	4494
Object	src_offsets	src_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4490.          int16 *src_offsets = NULL;
....
4494.              * (sizeof(*cells) + sizeof(*src_offsets) +
sizeof(*dst_offsets));
```

Use of Zero Initialized Pointer\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1241
Status	New

The variable declared in dst_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419 is not initialized when it is used by dst_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4419.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4491	4494
Object	dst_offsets	dst_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4491.          uint16 *dst_offsets = NULL;
....
4494.              * (sizeof(*cells) + sizeof(*src_offsets) +
sizeof(*dst_offsets));
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1242
Status	New

The variable declared in cells at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790 is not initialized when it is used by cells at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4794	4810
Object	cells	cells

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method copy_params_to_dynamic_space(WASMLoaderContext *loader_ctx, bool is_if_block,

```
....
4794.      uint8 *cells = NULL, cell;
....
4810.          size += sizeof(*cells) + sizeof(*src_offsets);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1243
Status	New

The variable declared in cells at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790 is not initialized when it is used by cells at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4794	4806
Object	cells	cells

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method copy_params_to_dynamic_space(WASMLoaderContext *loader_ctx, bool is_if_block,

```
....
4794.       uint8 *cells = NULL, cell;
....
4806.       uint64 size = (uint64)param_count * (sizeof(*cells) +
sizeof(*src_offsets));
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1244
Status	New

The variable declared in src_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790 is not initialized when it is used by src_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4795	4810
Object	src_offsets	src_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method copy_params_to_dynamic_space(WASMLoaderContext *loader_ctx, bool is_if_block,

```
....
4795.      int16 *src_offsets = NULL;
....
4810.          size += sizeof(*cells) + sizeof(*src_offsets);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1245
Status	New

The variable declared in src_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790 is not initialized when it is used by src_offsets at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4790.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4795	4806
Object	src_offsets	src_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method copy_params_to_dynamic_space(WASMLoaderContext *loader_ctx, bool is_if_block,

```
....
4795.      int16 *src_offsets = NULL;
....
4806.      uint64 size = (uint64)param_count * (sizeof(*cells) +
sizeof(*src_offsets));
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1246
Status	New

The variable declared in table_inst_linked at fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c in line 450 is not initialized when it is used by table_inst_linked at fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c in line 450.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	468	511

Object	table_inst_linked	table_inst_linked

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Method tables_instantiate(const WASMModule *module, WASMModuleInstance *module_inst,

```
....
468.          WASMTableInstance *table_inst_linked = NULL;
....
511.          table->table_inst_linked = table_inst_linked;
```

Use of Zero Initialized Pointer\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1247
Status New

The variable declared in linked_attachment at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 428 is not initialized when it is used by linked_func at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 428.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	439	450
Object	linked_attachment	linked_func

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
439.      void *linked_attachment = NULL;
....
450.      linked_func = wasm_native_resolve_symbol(
```

Use of Zero Initialized Pointer\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1248
Status New

The variable declared in linked_signature at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 428 is not initialized when it is used by linked_func at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 428.

	Source	Destination

File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	438	450
Object	linked_signature	linked_func

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
438.      const char *linked_signature = NULL;
....
450.      linked_func = wasm_native_resolve_symbol(
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1249
Status	New

The variable declared in import_functions at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668 is not initialized when it is used by import_functions at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	676	799
Object	import_functions	import_functions

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
676.      WASMImport *import_functions = NULL, *import_tables = NULL;
....
799.                        import = import_functions++;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1250
Status	New

The variable declared in import_memories at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668 is not initialized when it is used by import_memories at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	677	821
Object	import_memories	import_memories

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
677.      WASMImport *import_memories = NULL, *import_globals = NULL;
....
821.                        import = import_memories++;
```

Use of Zero Initialized Pointer\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1251
Status New

The variable declared in sub_module at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668 is not initialized when it is used by sub_module at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	768	847
Object	sub_module	sub_module

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
768.              WASMModule *sub_module = NULL;
....
847.              (void)sub_module;
```

Use of Zero Initialized Pointer\Path 39:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1252
Status	New

The variable declared in types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3820 is not initialized when it is used by types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3820.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	3835	3858
Object	types	types

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_emit_br_info(WASMLoaderContext *ctx, BranchBlock *frame_csp,

```
....
3835.      uint8 *types = NULL, cell;
....
3858.              cell = (uint8)wasm_value_type_cell_num(types[i]);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1253
Status	New

The variable declared in types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3820 is not initialized when it is used by types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3820.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	3835	3863
Object	types	types

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_emit_br_info(WASMLoaderContext *ctx, BranchBlock *frame_csp,

```
....
3835.      uint8 *types = NULL, cell;
....
3863.              cell = (uint8)wasm_value_type_cell_num(types[i]);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1254
Status	New

The variable declared in types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3820 is not initialized when it is used by types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3820.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	3835	3871
Object	types	types

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_emit_br_info(WASMLoaderContext *ctx, BranchBlock *frame_csp,

```
....
3835.      uint8 *types = NULL, cell;
....
3871.              cell = (uint8)wasm_value_type_cell_num(types[i]);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1255
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362 is not initialized when it is used by return_types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4369	4380
Object	return_types	return_types

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4369.      uint8 *return_types = NULL;
....
4380.          uint8 cell =
(uint8)wasm_value_type_cell_num(return_types[0]);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1256
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362 is not initialized when it is used by return_types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4369	4420
Object	return_types	return_types

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4369.      uint8 *return_types = NULL;
....
4420.          uint8 cells =
(uint8)wasm_value_type_cell_num(return_types[i]);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1257
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362 is not initialized when it is used by return_types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4369	4461
Object	return_types	return_types

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4369.      uint8 *return_types = NULL;
....
4461.              uint8 cell =
(uint8)wasm_value_type_cell_num(return_types[i]);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1258
Status	New

The variable declared in return_types at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362 is not initialized when it is used by dst_offsets at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4369	4470
Object	return_types	dst_offsets

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4369.      uint8 *return_types = NULL;
....
4470.                  dst_offsets[j] = dynamic_offset;
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1259
Status	New

The variable declared in src_offsets at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362 is not initialized when it is used by src_offsets at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c

Line	4433	4437
Object	src_offsets	src_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4433.          int16 *src_offsets = NULL;
....
4437.              * (sizeof(*cells) + sizeof(*src_offsets) +
sizeof(*dst_offsets));
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1260
Status	New

The variable declared in dst_offsets at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362 is not initialized when it is used by dst_offsets at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4362.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4434	4437
Object	dst_offsets	dst_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method reserve_block_ret(WASMLoaderContext *loader_ctx, uint8 opcode,

```
....
4434.          uint16 *dst_offsets = NULL;
....
4437.              * (sizeof(*cells) + sizeof(*src_offsets) +
sizeof(*dst_offsets));
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1261
Status	New

The variable declared in cells at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4733 is not initialized when it is used by cells at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4733.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4737	4753
Object	cells	cells

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method copy_params_to_dynamic_space(WASMLoaderContext *loader_ctx, bool is_if_block,

```
....
4737.      uint8 *cells = NULL, cell;
....
4753.          size += sizeof(*cells) + sizeof(*src_offsets);
```

Use of Zero Initialized Pointer\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1262
Status New

The variable declared in cells at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4733 is not initialized when it is used by cells at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4733.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4737	4749
Object	cells	cells

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method copy_params_to_dynamic_space(WASMLoaderContext *loader_ctx, bool is_if_block,

```
....
4737.      uint8 *cells = NULL, cell;
....
4749.      uint64 size = (uint64)param_count * (sizeof(*cells) +
sizeof(*src_offsets));
```

Use of Zero Initialized Pointer\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1263

Status	New

The variable declared in src_offsets at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4733 is not initialized when it is used by src_offsets at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4733.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4738	4753
Object	src_offsets	src_offsets

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method copy_params_to_dynamic_space(WASMLoaderContext *loader_ctx, bool is_if_block,

```
....
4738.      int16 *src_offsets = NULL;
....
4753.          size += sizeof(*cells) + sizeof(*src_offsets);
```

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=1000023&projectid=13&pathid=1136
Status	New

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Line	77	77
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Method static void rconf_section_entry_add(struct mk_rconf *conf,

```
....
77.      struct mk_rconf_entry *new;
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1137
Status	New

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Line	99	99
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Method struct mk_rconf_section *rconf_section_add(struct mk_rconf *conf,

```
....
99.      struct mk_rconf_section *new;
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1138
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Line	77	77
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Method static void rconf_section_entry_add(struct mk_rconf *conf,

```
....
77.      struct mk_rconf_entry *new;
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1139

Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Line	99	99
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Method struct mk_rconf_section *rconf_section_add(struct mk_rconf *conf,

```
....
99.      struct mk_rconf_section *new;
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1140
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Line	77	77
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Method static void rconf_section_entry_add(struct mk_rconf *conf,

```
....
77.      struct mk_rconf_entry *new;
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1141
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c

Line	99	99
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Method struct mk_rconf_section *rconf_section_add(struct mk_rconf *conf,

```
....
99.      struct mk_rconf_section *new;
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1142
Status New

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Line	77	77
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Method static void rconf_section_entry_add(struct mk_rconf *conf,

```
....
77.      struct mk_rconf_entry *new;
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1143
Status New

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Line	99	99
Object	neW	neW

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c

Method	struct mk_rconf_section *rconf_section_add(struct mk_rconf *conf,

```
....
99.      struct mk_rconf_section *new;
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1144
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	644	644
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method void storage_ext_init(StorageData* storage) {

```
....
644.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1145
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	335	335
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
335.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1146
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	463	463
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
463.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1147
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Line	514	514
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Method void storage_ext_init(StorageData* storage) {

```
....
514.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1148
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Line	284	284
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
284.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1149
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Line	391	391
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
391.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1150
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Line	285	285

Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
285.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1151
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Line	392	392
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
392.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1152
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Line	515	515
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Method void storage_ext_init(StorageData* storage) {

```
....
515.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1153
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Line	285	285
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
285.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1154
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Line	392	392
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
392.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 20:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1155
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Line	11	11
Object	nfc_dev	nfc_dev

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Method NfcDevice* nfc_device_alloc() {

```
....
11.      NfcDevice* nfc_dev = malloc(sizeof(NfcDevice));
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1156
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Line	237	237
Object	kv	kv

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Method bool nfc_device_load_mifare_df_key_settings(

```
....
237.                  MifareDesfireKeyVersion* kv =
malloc(sizeof(MifareDesfireKeyVersion));
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1157
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Line	618	618
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Method void storage_ext_init(StorageData* storage) {

```
....
618.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1158
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Line	323	323
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
323.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1159
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Line	450	450

Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
450.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1160
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Line	16	16
Object	nfc_dev	nfc_dev

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Method NfcDevice* nfc_device_alloc() {

```
....
16.      NfcDevice* nfc_dev = malloc(sizeof(NfcDevice));
```

Memory Leak\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1161
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Line	266	266
Object	kv	kv

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Method bool nfc_device_load_mifare_df_key_settings(

```
....
266.                    MifareDesfireKeyVersion* kv =
malloc(sizeof(MifareDesfireKeyVersion));
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1162
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Line	617	617
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Method void storage_ext_init(StorageData* storage) {

```
....
617.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1163
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Line	322	322
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
322.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1164
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Line	449	449
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
449.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1165
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	25	25
Object	picopass_worker	picopass_worker

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method PicopassWorker* picopass_worker_alloc() {

```
....
25.      PicopassWorker* picopass_worker =
malloc(sizeof(PicopassWorker));
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1166
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	22	22
Object	picopass_worker	picopass_worker

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method PicopassWorker* picopass_worker_alloc() {

```
....
22.      PicopassWorker* picopass_worker =
malloc(sizeof(PicopassWorker));
```

Memory Leak\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1167
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Line	624	624
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method void storage_ext_init(StorageData* storage) {

```
....
624.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1168
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c

Line	326	326
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
326.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1169
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Line	454	454
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
454.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1170
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	644	644
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c

Method	void storage_ext_init(StorageData* storage) {

```
....
644.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1171
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	335	335
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
335.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1172
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	463	463
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
463.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1173
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	644	644
Object	sd_data	sd_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method void storage_ext_init(StorageData* storage) {

```
....
644.      SDData* sd_data = malloc(sizeof(SDData));
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1174
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	335	335
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_file_open(

```
....
335.      SDFile* file_data = malloc(sizeof(SDFile));
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1175
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	463	463
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_open(void* ctx, File* file, const char* path) {

```
....
463.      SDDir* file_data = malloc(sizeof(SDDir));
```

Memory Leak\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1176
Status New

	Source	Destination
File	foxcpp@@maddy-v0.1.0-CVE-2022-24732-FP.c	foxcpp@@maddy-v0.1.0-CVE-2022-24732-FP.c
Line	16	16
Object	reply	reply

Code Snippet
File Name foxcpp@@maddy-v0.1.0-CVE-2022-24732-FP.c
Method struct error_obj run_pam_auth(const char *username, char *password) {

```
....
16.      struct pam_response *reply = malloc(sizeof(struct
pam_response));
```

Memory Leak\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1177
Status New

	Source	Destination
File	foxcpp@@maddy-v0.3.0-CVE-2022-24732-FP.c	foxcpp@@maddy-v0.3.0-CVE-2022-24732-FP.c
Line	16	16

Object	reply	reply

Code Snippet
File Name foxcpp@@maddy-v0.3.0-CVE-2022-24732-FP.c
Method struct error_obj run_pam_auth(const char *username, char *password) {

```
....
16.      struct pam_response *reply = malloc(sizeof(struct
pam_response));
```

Memory Leak\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1178
Status New

	Source	Destination
File	foxcpp@@maddy-v0.4.1-CVE-2022-24732-FP.c	foxcpp@@maddy-v0.4.1-CVE-2022-24732-FP.c
Line	34	34
Object	reply	reply

Code Snippet
File Name foxcpp@@maddy-v0.4.1-CVE-2022-24732-FP.c
Method struct error_obj run_pam_auth(const char *username, char *password) {

```
....
34.      struct pam_response *reply = malloc(sizeof(struct
pam_response));
```

Memory Leak\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1179
Status New

	Source	Destination
File	foxcpp@@maddy-v0.4.4-CVE-2022-24732-FP.c	foxcpp@@maddy-v0.4.4-CVE-2022-24732-FP.c
Line	34	34
Object	reply	reply

Code Snippet
File Name foxcpp@@maddy-v0.4.4-CVE-2022-24732-FP.c

Method	struct error_obj run_pam_auth(const char *username, char *password) {

```
....
34.      struct pam_response *reply = malloc(sizeof(struct
pam_response));
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1180
Status	New

	Source	Destination
File	foxcpp@@maddy-v0.5.0-CVE-2022-24732-TP.c	foxcpp@@maddy-v0.5.0-CVE-2022-24732-TP.c
Line	34	34
Object	reply	reply

Code Snippet	
File Name	foxcpp@@maddy-v0.5.0-CVE-2022-24732-TP.c
Method	struct error_obj run_pam_auth(const char *username, char *password) {

```
....
34.      struct pam_response *reply = malloc(sizeof(struct
pam_response));
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1181
Status	New

	Source	Destination
File	foxcpp@@maddy-v0.5.3-CVE-2022-24732-TP.c	foxcpp@@maddy-v0.5.3-CVE-2022-24732-TP.c
Line	34	34
Object	reply	reply

Code Snippet	
File Name	foxcpp@@maddy-v0.5.3-CVE-2022-24732-TP.c
Method	struct error_obj run_pam_auth(const char *username, char *password) {

```
....
34.      struct pam_response *reply = malloc(sizeof(struct
pam_response));
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1182
Status	New

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Line	197	197
Object	bitmapUpdate	bitmapUpdate

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Method BITMAP_UPDATE* update_read_bitmap_update(rdpUpdate* update, wStream* s)

```
....
197.        BITMAP_UPDATE* bitmapUpdate = calloc(1,
sizeof(BITMAP_UPDATE));
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1183
Status	New

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Line	261	261
Object	palette_update	palette_update

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Method PALETTE_UPDATE* update_read_palette(rdpUpdate* update, wStream* s)

```
....
261.        PALETTE_UPDATE* palette_update = calloc(1,
sizeof(PALETTE_UPDATE));
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1184
Status	New

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Line	325	325
Object	pointer_position	pointer_position

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Method POINTER_POSITION_UPDATE* update_read_pointer_position(rdpUpdate* update, wStream* s)

```
....
325.        POINTER_POSITION_UPDATE* pointer_position = calloc(1,
sizeof(POINTER_POSITION_UPDATE));
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1185
Status	New

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Line	343	343
Object	pointer_system	pointer_system

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11019-TP.c
Method POINTER_SYSTEM_UPDATE* update_read_pointer_system(rdpUpdate* update, wStream* s)

```
....
343.        POINTER_SYSTEM_UPDATE* pointer_system = calloc(1,
sizeof(POINTER_SYSTEM_UPDATE));
```

MemoryFree on StackVariable

Query Path:

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=279
Status	New

Calling free() (line 343) on a variable that was not dynamically allocated (line 343) in file flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	348	348
Object	file_data	file_data

Code Snippet

File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c

Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
348.        free(file_data);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=280
Status	New

Calling free() (line 470) on a variable that was not dynamically allocated (line 470) in file flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	476	476
Object	file_data	file_data

Code Snippet

File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c

Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
476.        free(file_data);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=281
Status	New

Calling free() (line 292) on a variable that was not dynamically allocated (line 292) in file flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Line	297	297
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
297.        free(file_data);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=282
Status	New

Calling free() (line 398) on a variable that was not dynamically allocated (line 398) in file flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Line	404	404
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
404.        free(file_data);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=283
Status	New

Calling free() (line 194) on a variable that was not dynamically allocated (line 194) in file flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24805-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24805-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24805-FP.c
Line	264	264
Object	instance	instance

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24805-FP.c
Method static void subghz_cli_command_rx(Cli* cli, string_t args, void* context) {

```
....
264.        free(instance);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=284
Status	New

Calling free() (line 194) on a variable that was not dynamically allocated (line 194) in file flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24807-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24807-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24807-FP.c
Line	264	264
Object	instance	instance

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24807-FP.c
Method static void subghz_cli_command_rx(Cli* cli, string_t args, void* context) {

```
....
264.        free(instance);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=285
Status	New

Calling free() (line 194) on a variable that was not dynamically allocated (line 194) in file flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24808-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24808-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24808-FP.c
Line	264	264
Object	instance	instance

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-24808-FP.c
Method static void subghz_cli_command_rx(Cli* cli, string_t args, void* context) {

```
....
264.        free(instance);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=286
Status	New

Calling free() (line 293) on a variable that was not dynamically allocated (line 293) in file flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Line	298	298
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
298.        free(file_data);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=287
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Line	405	405
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
405.        free(file_data);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=288
Status	New

Calling free() (line 293) on a variable that was not dynamically allocated (line 293) in file flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Line	298	298
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
298.        free(file_data);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=289
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Line	405	405
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
405.        free(file_data);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=290
Status	New

Calling free() (line 331) on a variable that was not dynamically allocated (line 331) in file flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Line	336	336
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
336.        free(file_data);
```

MemoryFree on StackVariable\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=291
Status	New

Calling free() (line 457) on a variable that was not dynamically allocated (line 457) in file flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Line	463	463
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
463.        free(file_data);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=292
Status	New

Calling free() (line 330) on a variable that was not dynamically allocated (line 330) in file flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Line	335	335
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
335.        free(file_data);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=293
Status	New

Calling free() (line 456) on a variable that was not dynamically allocated (line 456) in file flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Line	462	462
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
462.        free(file_data);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=294
Status	New

Calling free() (line 334) on a variable that was not dynamically allocated (line 334) in file flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Line	339	339
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
339.        free(file_data);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=295

Status	New

Calling free() (line 461) on a variable that was not dynamically allocated (line 461) in file flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Line	467	467
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
467.        free(file_data);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=296
Status	New

Calling free() (line 343) on a variable that was not dynamically allocated (line 343) in file flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	348	348
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
348.        free(file_data);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=297
Status	New

Calling free() (line 470) on a variable that was not dynamically allocated (line 470) in file flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	476	476
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
476.        free(file_data);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=298
Status New

Calling free() (line 343) on a variable that was not dynamically allocated (line 343) in file flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	348	348
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_file_close(void* ctx, File* file) {

```
....
348.        free(file_data);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=299
Status New

Calling free() (line 470) on a variable that was not dynamically allocated (line 470) in file flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	476	476
Object	file_data	file_data

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_close(void* ctx, File* file) {

```
....
476.        free(file_data);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=300
Status New

Calling free() (line 109) on a variable that was not dynamically allocated (line 109) in file fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c may result with a crash.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	122	122
Object	res1	res1

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method split_string(char *str, int *count)

```
....
122.                free(res1);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=301
Status New

Calling free() (line 146) on a variable that was not dynamically allocated (line 146) in file fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c may result with a crash.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	175	175
Object	cmd	cmd

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method app_instance_repl(wasm_module_inst_t module_inst)

```
....
175.        free(cmd);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=302
Status New

Calling free() (line 182) on a variable that was not dynamically allocated (line 182) in file FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c may result with a crash.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c
Line	251	251
Object	wszFormatName	wszFormatName

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c
Method wStream* cliprdr_packet_format_list_new(const CLIPRDR_FORMAT_LIST* formatList,

```
....
251.                            free(wszFormatName);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=303
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c may result with a crash.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Line	284	284
Object	PasswordHash	PasswordHash

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11086-TP.c
Method static int ntlm_convert_password_hash(NTLM_CONTEXT* context, BYTE* hash)

```
....
284.        free(PasswordHash);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=304
Status New

Calling free() (line 810) on a variable that was not dynamically allocated (line 810) in file FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c may result with a crash.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	960	960
Object	serial	serial

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method UINT DeviceServiceEntry(PDEVICE_SERVICE_ENTRY_POINTS pEntryPoints)

```
....
960.        free(serial);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=305
Status New

Calling free() (line 484) on a variable that was not dynamically allocated (line 484) in file FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c may result with a crash.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	508	508
Object	data	data

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method static DWORD WINAPI irp_thread_func(LPVOID arg)

```
....
508.         free(data);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=306
Status New

Calling free() (line 513) on a variable that was not dynamically allocated (line 513) in file FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c may result with a crash.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	578	578
Object	ids	ids

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method static void create_irp_thread(SERIAL_DEVICE* serial, IRP* irp)

```
....
578.                 free(ids);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=307
Status New

Calling free() (line 667) on a variable that was not dynamically allocated (line 667) in file FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c may result with a crash.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	692	692
Object	ids	ids

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method static void terminate_pending_irp_threads(SERIAL_DEVICE* serial)

```
....
692.         free(ids);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=308
Status New

Calling free() (line 769) on a variable that was not dynamically allocated (line 769) in file FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c may result with a crash.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	793	793
Object	serial	serial

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method static UINT serial_free(DEVICE* device)

```
....
793.         free(serial);
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

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

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=309
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Line	264	264
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
264.              temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=310
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Line	266	266
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
266.              temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=311
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 244 of flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Line	254	254
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
254.              temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=312
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 244 of flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Line	256	256
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
256.              temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 5:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=313
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Line	264	264
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
264.                temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=314
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Line	266	266
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
266.                temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=315
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 253 of flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c
Line	263	263
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
263.              temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=316
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 253 of flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c
Line	265	265
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
265.              temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=317
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Line	264	264
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
264.              temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=318
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Line	266	266
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
266.              temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=319
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Line	264	264
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
264.                temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=320
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Line	266	266
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
266.                temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=321

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Line	264	264
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
264.              temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=322
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 254 of flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Line	266	266
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
266.              temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=323
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 255 of flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Line	265	265
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
265.              temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=324
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 255 of flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Line	267	267
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
267.              temp[temp_loc++] = digit - 10 + 'A';
```

Char Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=325
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 259 of flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Line	269	269
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
269.              temp[temp_loc++] = digit + '0';
```

Char Overflow\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=326
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 259 of flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Line	271	271
Object	AssignExpr	AssignExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
271.              temp[temp_loc++] = digit - 10 + 'A';
```

Buffer Overflow AddressOfLocalVarReturned

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=8
Status	New

The pointer __heap_end__ at flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c in line 548 is being used after it has been freed.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Line	549	549
Object	__heap_end__	__heap_end__

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Method size_t xPortGetTotalHeapSize(void) {

```
....
549.      return (size_t)&__heap_end__ - (size_t)&__heap_start__;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=9
Status	New

The pointer __heap_start__ at flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c in line 548 is being used after it has been freed.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Line	549	549
Object	__heap_start__	__heap_start__

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Method size_t xPortGetTotalHeapSize(void) {

```
....
549.      return (size_t)&__heap_end__ - (size_t)&__heap_start__;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=10
Status	New

The pointer type_str at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 206 is being used after it has been freed.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	211	211
Object	type_str	type_str

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method type2str(uint8 type)

```
....
211.          return type_str[type - VALUE_TYPE_V128];
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=11
Status	New

The pointer p_end at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 296 is being used after it has been freed.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	357	357
Object	p_end	p_end

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method check_utf8_str(const uint8 *str, uint32 len)

```
....
357.      return (p == p_end);
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=12
Status	New

The pointer type_str at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 206 is being used after it has been freed.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	211	211
Object	type_str	type_str

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method type2str(uint8 type)

```
....
211.          return type_str[type - VALUE_TYPE_V128];
```

Buffer Overflow AddressOfLocalVarReturned\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=13
Status	New

The pointer p_end at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 296 is being used after it has been freed.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	357	357
Object	p_end	p_end

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method check_utf8_str(const uint8 *str, uint32 len)

```
....
357.      return (p == p_end);
```

Heap Inspection

Query Path:

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=1000023&projectid=13&pathid=1131
Status	New

Method basic_auth_start at line 615 of flatpak@@flatpak-1.12.3-CVE-2023-28101-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	flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c	flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c
Line	622	622
Object	password	password

Code Snippet
File Name flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c
Method basic_auth_start (FlatpakTransaction *transaction,

```
....
622.    char *user, *password, *previous_error = NULL;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1132
Status	New

Method basic_auth_start at line 666 of flatpak@@flatpak-1.15.0-CVE-2023-28101-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	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Line	673	673
Object	password	password

Code Snippet
File Name flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Method basic_auth_start (FlatpakTransaction *transaction,

```
....
673.    char *user, *password, *previous_error = NULL;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1133
Status	New

Method basic_auth_start at line 666 of flatpak@@flatpak-1.15.2-CVE-2023-28101-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	flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c
Line	673	673
Object	password	password

Code Snippet
File Name flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c
Method basic_auth_start (FlatpakTransaction *transaction,

```
....
673.    char *user, *password, *previous_error = NULL;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1134
Status	New

Method basic_auth_start at line 667 of flatpak@@flatpak-1.15.6-CVE-2023-28101-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	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Line	674	674
Object	password	password

Code Snippet

File Name	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Method	basic_auth_start (FlatpakTransaction *transaction,

```
....
674.    char *user, *password, *previous_error = NULL;
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1135
Status	New

Method basic_auth_start at line 667 of flatpak@@flatpak-1.15.9-CVE-2023-28101-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	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Line	674	674
Object	password	password

Code Snippet

File Name	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Method	basic_auth_start (FlatpakTransaction *transaction,

```
....
674.    char *user, *password, *previous_error = NULL;
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1210
Status	New

The variable declared in serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810 is not initialized when it is used by serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810.

	Source	Destination

File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	818	958
Object	serial	serial

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method UINT DeviceServiceEntry(PDEVICE_SERVICE_ENTRY_POINTS pEntryPoints)

```
....
818.        SERIAL_DEVICE* serial;
....
958.        MessageQueue_Free(serial->MainIrpQueue);
```

Use of Uninitialized Pointer\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1211
Status New

The variable declared in serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810 is not initialized when it is used by serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	818	957
Object	serial	serial

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method UINT DeviceServiceEntry(PDEVICE_SERVICE_ENTRY_POINTS pEntryPoints)

```
....
818.        SERIAL_DEVICE* serial;
....
957.        ListDictionary_Free(serial->IrpThreads);
```

Use of Uninitialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1212
Status New

The variable declared in serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810 is not initialized when it is used by serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	818	959
Object	serial	serial

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method UINT DeviceServiceEntry(PDEVICE_SERVICE_ENTRY_POINTS pEntryPoints)

```
....
818.        SERIAL_DEVICE* serial;
....
959.        Stream_Free(serial->device.data, TRUE);
```

Use of Uninitialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1213
Status New

The variable declared in serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810 is not initialized when it is used by serial at FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c in line 810.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	818	960
Object	serial	serial

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method UINT DeviceServiceEntry(PDEVICE_SERVICE_ENTRY_POINTS pEntryPoints)

```
....
818.        SERIAL_DEVICE* serial;
....
960.        free(serial);
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=277
Status	New

The application performs an illegal operation in HAL_DCMI_Start_DMA, in flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c. In line 467, the program attempts to divide by circular_copy_length, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input circular_copy_length in HAL_DCMI_Start_DMA of flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c, at line 467.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c
Line	538	538
Object	circular_copy_length	circular_copy_length

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c
Method HAL_StatusTypeDef HAL_DCMI_Start_DMA(DCMI_HandleTypeDef* hdcmi, uint32_t DCMI_Mode, uint32_t pData, uint32_t Length)

```
....
538.      hdcmi->XferCount = 2U * ((Length / circular_copy_length) -
1U);
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=278
Status	New

The application performs an illegal operation in HAL_DCMI_Start_DMA, in flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c. In line 467, the program attempts to divide by circular_copy_length, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input circular_copy_length in HAL_DCMI_Start_DMA of flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c, at line 467.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c
Line	549	549
Object	circular_copy_length	circular_copy_length

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.1.0-CVE-2021-3520-FP.c
Method HAL_StatusTypeDef HAL_DCMI_Start_DMA(DCMI_HandleTypeDef* hdcmi, uint32_t DCMI_Mode, uint32_t pData, uint32_t Length)

```
....
549.      hdcmi->pCircularBuffer +=  4U * (((Length /
circular_copy_length) - 1U) * circular_copy_length);
```

Download of Code Without Integrity Check

Query Path:
CPP\Cx\CPP Medium Threat\Download of Code Without Integrity Check Version:1

Categories

FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Download of Code Without Integrity Check\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1208
Status	New

The method main in the file fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c at line 297 remotely loads and executes code without running an integrity check, leaving it vulnerable to potential attack.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	297	214
Object	argv	dlopen

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
297.  main(int argc, char *argv[])
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method load_and_register_native_libs(const char **native_lib_list,

```
....
214.          if (!(handle = dlopen(native_lib_list[i], RTLD_NOW |
RTLD_GLOBAL))
```

Download of Code Without Integrity Check\Path 2:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1209
Status	New

The method main in the file fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c at line 297 remotely loads and executes code without running an integrity check, leaving it vulnerable to potential attack.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	297	215
Object	argv	dlopen

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
297.  main(int argc, char *argv[])
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method load_and_register_native_libs(const char **native_lib_list,

```
....
215.              && !(handle = dlopen(native_lib_list[i], RTLD_LAZY)))
{
```

Wrong Memory Allocation

Query Path:
CPP\Cx\CPP Medium Threat\Wrong Memory Allocation Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description
Wrong Memory Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1558
Status	New

The function malloc in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c at line 497 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination

File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Line	508	508
Object	sizeof	malloc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-40363-TP.c
Method bool nfc_device_load_mifare_df_data(FlipperFormat* file, NfcDevice* dev) {

```
....
508.              data->free_memory =
malloc(sizeof(MifareDesfireFreeMemory));
```

Wrong Memory Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1559
Status	New

The function malloc in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c at line 529 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Line	540	540
Object	sizeof	malloc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-40363-TP.c
Method bool nfc_device_load_mifare_df_data(FlipperFormat* file, NfcDevice* dev) {

```
....
540.              data->free_memory =
malloc(sizeof(MifareDesfireFreeMemory));
```

Stored Buffer Overflow fgets

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow fgets Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Stored Buffer Overflow fgets\Path 1:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1560
Status	New

The size of the buffer used by ares__read_line in bytestoread, at line 41 of fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ares__read_line passes to BinaryExpr, at line 41 of fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c
Line	58	58
Object	BinaryExpr	bytestoread

Code Snippet
File Name fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c
Method ares_status_t ares__read_line(FILE *fp, char **buf, size_t *bufsize)

```
....
58.      if (!fgets(*buf + offset, bytestoread, fp)) {
```

Stored Buffer Overflow fgets\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1561
Status	New

The size of the buffer used by ares__read_line in bytestoread, at line 41 of fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ares__read_line passes to BinaryExpr, at line 41 of fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c, to overwrite the target buffer.

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c
Line	58	58
Object	BinaryExpr	bytestoread

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c
Method ares_status_t ares__read_line(FILE *fp, char **buf, size_t *bufsize)

```
....
58.      if (!fgets(*buf + offset, bytestoread, fp)) {
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=327
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 182 of FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c
Line	296	296
Object	AssignExpr	AssignExpr

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11085-TP.c
Method wStream* cliprdr_packet_format_list_new(const CLIPRDR_FORMAT_LIST* formatList,

```
....
296.                            cchWideChar = (int)(rem / 2);
```

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=1000023&projectid=13&pathid=1590
Status	New

The storage_ext_dir_read method calls the snprintf function, at line 480 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Line	501	501
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
501.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1591
Status New

The storage_ext_dir_read method calls the snprintf function, at line 408 of flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Line	429	429
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
429.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1592
Status New

The storage_ext_dir_read method calls the snprintf function, at line 409 of flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Line	430	430
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
430.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1593
Status New

The storage_ext_dir_read method calls the snprintf function, at line 409 of flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Line	430	430
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
430.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1594

Status	New

The storage_ext_dir_read method calls the snprintf function, at line 467 of flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Line	488	488
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
488.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1595
Status	New

The storage_ext_dir_read method calls the snprintf function, at line 466 of flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Line	487	487
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
487.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1596
Status	New

The storage_ext_dir_read method calls the snprintf function, at line 471 of flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Line	492	492
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
492.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1597
Status	New

The storage_ext_dir_read method calls the snprintf function, at line 480 of flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Line	501	501
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
501.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1598
Status	New

The storage_ext_dir_read method calls the snprintf function, at line 480 of flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Line	501	501
Object	snprintf	snprintf

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2022-38890-FP.c
Method static bool storage_ext_dir_read(

```
....
501.          snprintf(name, name_length, "%s", _fileinfo.fname);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1599
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.          return malloc(size);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1600
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1601
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1602
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1603
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1604
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1605
Status	New

The module_reader_callback method calls the snprintf function, at line 261 of fluent@@fluent-bit-v2.0.14-CVE-2023-48105-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	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	272	272
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method module_reader_callback(const char *module_name, uint8 **p_buffer,

```
....
272.      snprintf(wasm_file_name, sz, format, module_search_path,
module_name);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1606
Status	New

The set_error_buf method calls the snprintf function, at line 26 of fluent@@fluent-bit-v2.0.14-CVE-2023-52284-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	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	29	29
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method set_error_buf(char *error_buf, uint32 error_buf_size, const char *string)

```
....
29.          snprintf(error_buf, error_buf_size, "WASM module load
failed: %s",
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1607
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1608
Status	New

The uint32 method calls the snprintf function, at line 2652 of fluent@@fluent-bit-v2.0.5-CVE-2023-48105-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	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	2671	2671
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Method uint32

```
....
2671.
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1609
Status	New

The uint32 method calls the snprintf function, at line 2652 of fluent@@fluent-bit-v2.0.5-CVE-2023-48105-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	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	2705	2705
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c

Method	uint32

```
....
2705.      }
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1610
Status	New

The set_error_buf method calls the snprintf function, at line 24 of fluent@@fluent-bit-v2.0.5-CVE-2023-48105-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	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	27	27
Object	snprintf	snprintf

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Method	set_error_buf(char *error_buf, uint32 error_buf_size, const char *string)

```
....
27.          snprintf(error_buf, error_buf_size,
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1611
Status	New

The set_error_buf_v method calls the snprintf function, at line 33 of fluent@@fluent-bit-v2.0.5-CVE-2023-48105-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	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	42	42
Object	snprintf	snprintf

Code Snippet

File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Method	set_error_buf_v(char *error_buf, uint32 error_buf_size, const char *format, ...)

```
....
42.          snprintf(error_buf, error_buf_size,
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1612
Status	New

The wasm_set_exception method calls the snprintf function, at line 1800 of fluent@@fluent-bit-v2.0.5-CVE-2023-48105-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	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	1803	1803
Object	snprintf	snprintf

Code Snippet

File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Method	wasm_set_exception(WASMModuleInstance *module_inst, const char *exception)

```
....
1803.          snprintf(module_inst->cur_exception, sizeof(module_inst-
>cur_exception),
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1613
Status	New

The set_error_buf method calls the snprintf function, at line 26 of fluent@@fluent-bit-v2.0.5-CVE-2023-52284-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	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	29	29
Object	snprintf	snprintf

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	set_error_buf(char *error_buf, uint32 error_buf_size, const char *string)

```
....
29.          snprintf(error_buf, error_buf_size, "WASM module load
failed: %s",
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1614
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet	
File Name	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Method	system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1615
Status	New

The wasm_loader_prepare_bytecode method calls the snprintf function, at line 7197 of fluent@@fluent-bit-v2.1.9-CVE-2023-48105-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	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	9899	9899

Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
9899.                                   snprintf(error_buf, error_buf_size,
```

Unchecked Return Value\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1616
Status New

The set_error_buf method calls the snprintf function, at line 32 of fluent@@fluent-bit-v2.1.9-CVE-2023-48105-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	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	35	35
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method set_error_buf(char *error_buf, uint32 error_buf_size, const char *string)

```
....
35.          snprintf(error_buf, error_buf_size, "WASM module load
failed: %s",
```

Unchecked Return Value\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1617
Status New

The set_error_buf_v method calls the snprintf function, at line 41 of fluent@@fluent-bit-v2.1.9-CVE-2023-48105-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	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c

Line	50	50
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method set_error_buf_v(char *error_buf, uint32 error_buf_size, const char *format, ...)

```
....
50.          snprintf(error_buf, error_buf_size, "WASM module load
failed: %s", buf);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1618
Status	New

The init_llvm_jit_functions_stage2 method calls the snprintf function, at line 3074 of fluent@@fluent-bit-v2.1.9-CVE-2023-48105-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	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	3102	3102
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method init_llvm_jit_functions_stage2(WASMModule *module, char *error_buf,

```
....
3102.          snprintf(func_name, sizeof(func_name), "%s%d",
AOT_FUNC_PREFIX, i);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1619
Status	New

The orcjit_thread_callback method calls the snprintf function, at line 3161 of fluent@@fluent-bit-v2.1.9-CVE-2023-48105-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	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	3247	3247
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method orcjit_thread_callback(void *arg)

```
....
3247.           snprintf(func_name, sizeof(func_name), "%s%d%s",
AOT_FUNC_PREFIX, i,
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1620
Status	New

The orcjit_thread_callback method calls the snprintf function, at line 3161 of fluent@@fluent-bit-v2.1.9-CVE-2023-48105-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	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	3269	3269
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method orcjit_thread_callback(void *arg)

```
....
3269.                   snprintf(func_name, sizeof(func_name), "%s%d",
AOT_FUNC_PREFIX,
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1621
Status	New

The wasm_loader_prepare_bytecode method calls the snprintf function, at line 7197 of fluent@@fluent-bit-v2.1.9-CVE-2023-52284-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	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	9899	9899
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
9899.                                   snprintf(error_buf, error_buf_size,
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1622
Status New

The set_error_buf method calls the snprintf function, at line 32 of fluent@@fluent-bit-v2.1.9-CVE-2023-52284-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	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	35	35
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method set_error_buf(char *error_buf, uint32 error_buf_size, const char *string)

```
....
35.          snprintf(error_buf, error_buf_size, "WASM module load
failed: %s",
```

Unchecked Return Value\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1623
Status New

The set_error_buf_v method calls the snprintf function, at line 41 of fluent@@fluent-bit-v2.1.9-CVE-2023-52284-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	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	50	50
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method set_error_buf_v(char *error_buf, uint32 error_buf_size, const char *format, ...)

```
....
50.          snprintf(error_buf, error_buf_size, "WASM module load
failed: %s", buf);
```

Unchecked Return Value\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1624
Status New

The init_llvm_jit_functions_stage2 method calls the snprintf function, at line 3074 of fluent@@fluent-bit-v2.1.9-CVE-2023-52284-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	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	3102	3102
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method init_llvm_jit_functions_stage2(WASMModule *module, char *error_buf,

```
....
3102.          snprintf(func_name, sizeof(func_name), "%s%d",
AOT_FUNC_PREFIX, i);
```

Unchecked Return Value\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1625
Status	New

The orcjit_thread_callback method calls the snprintf function, at line 3161 of fluent@@fluent-bit-v2.1.9-CVE-2023-52284-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	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	3247	3247
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method orcjit_thread_callback(void *arg)

```
....
3247.           snprintf(func_name, sizeof(func_name), "%s%d%s",
AOT_FUNC_PREFIX, i,
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1626
Status	New

The orcjit_thread_callback method calls the snprintf function, at line 3161 of fluent@@fluent-bit-v2.1.9-CVE-2023-52284-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	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	3269	3269
Object	snprintf	snprintf

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method orcjit_thread_callback(void *arg)

```
....
3269.                   snprintf(func_name, sizeof(func_name), "%s%d",
AOT_FUNC_PREFIX,
```

Unchecked Return Value\Path 38:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1627
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1628
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1629
Status	New

The system_alloc method calls the malloc function, at line 151 of fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Line	154	154
Object	malloc	malloc

Code Snippet
File Name fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1630
Status	New

The *sim_subtype2name method calls the snprintf function, at line 464 of FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-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	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c
Line	467	467
Object	snprintf	snprintf

Code Snippet
File Name FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c
Method char const *sim_subtype2name(enum eapsim_subtype subtype, char *subtypenamebuf, int subtypenamebuflen)

```
....
467.              snprintf(subtypenamebuf, subtypenamebuflen, "illegal-
subtype:%d", subtype);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1631
Status	New

The *sim_state2name method calls the snprintf function, at line 442 of FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-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	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c
Line	447	447
Object	snprintf	snprintf

Code Snippet
File Name FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41860-TP.c
Method char const *sim_state2name(enum eapsim_clientstates state,

```
....
447.              snprintf(statenamebuf, statenamebuflen, "eapstate:%d",
state);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1632
Status	New

The subghz_on_system_start method calls the arg function, at line 1243 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c
Line	1280	1280
Object	arg	arg

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c
Method void subghz_on_system_start(void) {

```
....
1280.          pb_region.bands.arg = malloc(sizeof(FuriHalRegion));
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1633
Status	New

The subghz_on_system_start_istream_decode_band method calls the region function, at line 1209 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c
Line	1223	1223
Object	region	region

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24805-FP.c
Method static bool subghz_on_system_start_istream_decode_band(

```
....
1223.      region = realloc( //-V701
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1634
Status	New

The subghz_on_system_start method calls the arg function, at line 1243 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c
Line	1280	1280
Object	arg	arg

Code Snippet	
File Name	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c
Method	void subghz_on_system_start(void) {

```
....
1280.          pb_region.bands.arg = malloc(sizeof(FuriHalRegion));
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1635
Status	New

The subghz_on_system_start_istream_decode_band method calls the region function, at line 1209 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c
Line	1223	1223
Object	region	region

Code Snippet	
File Name	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24807-FP.c
Method	static bool subghz_on_system_start_istream_decode_band(

```
....
1223.      region = realloc( //-V701
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1636
Status	New

The subghz_on_system_start method calls the arg function, at line 1243 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c
Line	1280	1280

Object	arg	arg

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c
Method void subghz_on_system_start(void) {

```
....
1280.          pb_region.bands.arg = malloc(sizeof(FuriHalRegion));
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1637
Status	New

The subghz_on_system_start_istream_decode_band method calls the region function, at line 1209 of flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c
Line	1223	1223
Object	region	region

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2022-24808-FP.c
Method static bool subghz_on_system_start_istream_decode_band(

```
....
1223.      region = realloc( //-V701
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1638
Status	New

The sd_format_card method calls the work_area function, at line 111 of flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c

Line	118	118
Object	work_area	work_area

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2022-38890-FP.c
Method FS_Error sd_format_card(StorageData* storage) {

```
....
118.      work_area = malloc(_MAX_SS);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1639
Status	New

The sd_format_card method calls the work_area function, at line 112 of flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Line	119	119
Object	work_area	work_area

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2022-38890-FP.c
Method FS_Error sd_format_card(StorageData* storage) {

```
....
119.      work_area = malloc(_MAX_SS);
```

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=1000023&projectid=13&pathid=1797
Status	New

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-	fluent@@fluent-bit-tiger-1.8.15-

	20230223-CVE-2022-48468-TP.c	20230223-CVE-2022-48468-TP.c
Line	3497	3541
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3497.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3541.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1798
Status New

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Line	3497	3541
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3497.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3541.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1799
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Line	3497	3541
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3497.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3541.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1800
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Line	3497	3541
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3497.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3541.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1801
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Line	3497	3541
Object	GenericHandler	sizeof

Code Snippet

File Name fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c

Method typedef void (*GenericHandler) (void *service,

```
....
3497.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3541.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1802
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Line	3502	3546
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3502.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3546.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1803
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Line	3502	3546
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3502.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3546.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1804
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Line	3502	3546
Object	GenericHandler	sizeof

Code Snippet

File Name fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c

Method typedef void (*GenericHandler) (void *service,

```
....
3502.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3546.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1805
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Line	3502	3546
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3502.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3546.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1806
Status New

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Line	3502	3546
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3502.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3546.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1807
Status	New

	Source	Destination
File	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Line	3497	3541
Object	GenericHandler	sizeof

Code Snippet
File Name fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3497.  typedef void (*GenericHandler) (void *service,
```

File Name fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3541.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1808
Status	New

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Line	1260	1260
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1260.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1809
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.3.6-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.3.6-CVE-2024-4323-FP.c
Line	241	241
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.3.6-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
241.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1810
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.3.6-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.3.6-CVE-2024-4323-FP.c
Line	299	299
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.3.6-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
299.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1811
Status	New

	Source	Destination

File	fluent@@fluent-bit-v1.4.3-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.4.3-CVE-2024-4323-FP.c
Line	241	241
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.4.3-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
241.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1812
Status New

	Source	Destination
File	fluent@@fluent-bit-v1.4.3-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.4.3-CVE-2024-4323-FP.c
Line	299	299
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.4.3-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
299.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1813
Status New

	Source	Destination
File	fluent@@fluent-bit-v1.5.3-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.5.3-CVE-2024-4323-FP.c
Line	299	299
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.5.3-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
299.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1814
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.5.3-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.5.3-CVE-2024-4323-FP.c
Line	357	357
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.5.3-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
357.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1815
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.6.5-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.6.5-CVE-2024-4323-FP.c
Line	299	299
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.6.5-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
299.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1816
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.6.5-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.6.5-CVE-2024-4323-FP.c
Line	357	357
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.6.5-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
357.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1817
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.7.2-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.7.2-CVE-2024-4323-FP.c
Line	306	306
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.7.2-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
306.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1818

Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.7.2-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.7.2-CVE-2024-4323-FP.c
Line	376	376
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.7.2-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
376.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1819
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Line	1260	1260
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1260.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1820
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c

Line	1260	1260
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1260.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1821
Status New

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Line	1260	1260
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1260.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1822
Status New

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.9.3-CVE-2024-4323-FP.c
Line	342	342
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.9.3-CVE-2024-4323-FP.c

Method	void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
342.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1823
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.9.3-CVE-2024-4323-FP.c
Line	416	416
Object	sizeof	sizeof

Code Snippet

File Name	fluent@@fluent-bit-v1.9.3-CVE-2024-4323-FP.c
Method	void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
416.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1824
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Line	1260	1260
Object	sizeof	sizeof

Code Snippet

File Name	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Method	sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1260.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1825
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.9.7-CVE-2024-4323-FP.c
Line	342	342
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.9.7-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
342.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1826
Status	New

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.9.7-CVE-2024-4323-FP.c
Line	416	416
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v1.9.7-CVE-2024-4323-FP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
416.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1827
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Line	1259	1259
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1259.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1828
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	120	120
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method split_string(char *str, int *count)

```
....
120.          res = (char **)realloc(res1, sizeof(char *) * (uint32)(idx
+ 1));
```

Use of Sizeof On a Pointer Type\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1829
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	378	378

Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
378.              if (dir_list_size >= sizeof(dir_list) / sizeof(char
*)) {
```

Use of Sizeof On a Pointer Type\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1830
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	380	380
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
380.                          (int)(sizeof(dir_list) / sizeof(char *)));
```

Use of Sizeof On a Pointer Type\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1831
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	390	390
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
390.              if (env_list_size >= sizeof(env_list) / sizeof(char
*)) {
```

Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1832
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	392	392
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
392.                          (int)(sizeof(env_list) / sizeof(char *)));
```

Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1833
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	415	415
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
415.                  if (addr_pool_size >= sizeof(addr_pool) /
sizeof(char *)) {
```

Use of Sizeof On a Pointer Type\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1834
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	417	417
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
417.                                (int)(sizeof(addr_pool) / sizeof(char
*)));
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1835
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	442	442
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
442.              if (native_lib_count >= sizeof(native_lib_list) /
sizeof(char *)) {
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1836
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	444	444
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
444.                          (int)(sizeof(native_lib_list) / sizeof(char
*)));
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1837
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	357	357
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_type_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
357.          total_size = sizeof(WASMType *) * (uint64)type_count;
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1838
Status	New

	Source	Destination

File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	953	953
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_function_section(const uint8 *buf, const uint8 *buf_end,

```
....
953.          total_size = sizeof(WASMFunction *) * (uint64)func_count;
```

Use of Sizeof On a Pointer Type\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1839
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	1515	1515
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_data_segment_section(const uint8 *buf, const uint8 *buf_end,

```
....
1515.          total_size = sizeof(WASMDataSeg *) *
(uint64)data_seg_count;
```

Use of Sizeof On a Pointer Type\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1840
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	2190	2190
Object	sizeof	sizeof

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	load_from_sections(WASMModule *module, WASMSection *sections,

```
....
2190.                loader_malloc(sizeof(void *) * module-
>function_count, error_buf,
```

Use of Sizeof On a Pointer Type\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1841
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	3702	3702
Object	sizeof	sizeof

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	wasm_loader_emit_ptr(WASMLoaderContext *ctx, void *value)

```
....
3702.          ctx->p_code_compiled += sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1842
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	3708	3708
Object	sizeof	sizeof

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	wasm_loader_emit_ptr(WASMLoaderContext *ctx, void *value)

```
....
3708.          increase_compiled_code_space(ctx, sizeof(void *));
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1843
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	5609	5609
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
5609.                                                - sizeof(void *)) =
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1844
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	5694	5694
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
5694.                       *(void **)(p_code_compiled_tmp - sizeof(void
*)) =
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1845
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2024-4323-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2024-4323-TP.c
Line	342	342
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2024-4323-TP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
342.      metrics_arr = flb_malloc(num_metrics * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1846
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2024-4323-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2024-4323-TP.c
Line	416	416
Object	sizeof	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2024-4323-TP.c
Method void cb_metrics_prometheus(mk_request_t *request, void *data)

```
....
416.      qsort(metrics_arr, num_metrics, sizeof(char *), string_cmp);
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1440
Status	New

The variable declared in null at flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c in line 152 is not initialized when it is used by message at flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c in line 152.

	Source	Destination
File	flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c	flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c
Line	158	174
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.12.3-CVE-2023-28101-TP.c
Method install_authenticator (FlatpakTransaction *old_transaction,

```
....
158.    g_autoptr(GError) local_error = NULL;
....
174.        g_printerr ("Unable to install authenticator: %s\n",
local_error->message);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1441
Status	New

The variable declared in null at flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c in line 154 is not initialized when it is used by message at flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c in line 154.

	Source	Destination
File	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Line	160	176
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Method install_authenticator (FlatpakTransaction *old_transaction,

```
....
160.    g_autoptr(GError) local_error = NULL;
....
176.        g_printerr ("Unable to install authenticator: %s\n",
local_error->message);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1442
Status	New

The variable declared in null at flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c in line 821 is not initialized when it is used by message at flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c in line 821.

	Source	Destination
File	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Line	828	845
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
828.    g_autoptr(GError) local_error = NULL;
....
845.                    flatpak_decomposed_get_ref (ref), local_error-
>message);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1443
Status	New

The variable declared in null at flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c in line 821 is not initialized when it is used by message at flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c in line 821.

	Source	Destination
File	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Line	828	857
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.0-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
828.    g_autoptr(GError) local_error = NULL;
....
857.                      flatpak_decomposed_get_ref (ref), local_error-
>message);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1444
Status	New

The variable declared in null at flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c in line 154 is not initialized when it is used by message at flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c in line 154.

	Source	Destination
File	flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c
Line	160	176
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c
Method install_authenticator (FlatpakTransaction *old_transaction,

```
....
160.    g_autoptr(GError) local_error = NULL;
....
176.        g_printerr ("Unable to install authenticator: %s\n",
local_error->message);
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1445
Status	New

The variable declared in null at flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c in line 821 is not initialized when it is used by message at flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c in line 821.

	Source	Destination
File	flatpak@@flatpak-1.15.2-CVE-2023-	flatpak@@flatpak-1.15.2-CVE-2023-

	28101-TP.c	28101-TP.c
Line	828	845
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
828.    g_autoptr(GError) local_error = NULL;
....
845.                    flatpak_decomposed_get_ref (ref), local_error-
>message);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1446
Status	New

The variable declared in null at flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c in line 821 is not initialized when it is used by message at flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c in line 821.

	Source	Destination
File	flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c
Line	828	857
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.2-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
828.    g_autoptr(GError) local_error = NULL;
....
857.                    flatpak_decomposed_get_ref (ref), local_error-
>message);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1447
Status	New

The variable declared in null at flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c in line 155 is not initialized when it is used by message at flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c in line 155.

	Source	Destination
File	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Line	161	177
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Method install_authenticator (FlatpakTransaction *old_transaction,

```
....
161.    g_autoptr(GError) local_error = NULL;
....
177.        g_printerr ("Unable to install authenticator: %s\n",
local_error->message);
```

NULL Pointer Dereference\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1448
Status New

The variable declared in null at flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c in line 825 is not initialized when it is used by message at flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c in line 825.

	Source	Destination
File	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Line	832	849
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
832.    g_autoptr(GError) local_error = NULL;
....
849.                    flatpak_decomposed_get_ref (ref), local_error-
>message);
```

NULL Pointer Dereference\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1449
Status	New

The variable declared in null at flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c in line 825 is not initialized when it is used by message at flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c in line 825.

	Source	Destination
File	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Line	832	861
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.6-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
832.    g_autoptr(GError) local_error = NULL;
....
861.                    flatpak_decomposed_get_ref (ref), local_error->message);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1450
Status	New

The variable declared in null at flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c in line 155 is not initialized when it is used by message at flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c in line 155.

	Source	Destination
File	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Line	161	177
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Method install_authenticator (FlatpakTransaction *old_transaction,

```
....
161.    g_autoptr(GError) local_error = NULL;
....
177.        g_printerr ("Unable to install authenticator: %s\n", local_error->message);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1451
Status	New

The variable declared in null at flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c in line 825 is not initialized when it is used by message at flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c in line 825.

	Source	Destination
File	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Line	832	849
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
832.    g_autoptr(GError) local_error = NULL;
....
849.                    flatpak_decomposed_get_ref (ref), local_error->message);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1452
Status	New

The variable declared in null at flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c in line 825 is not initialized when it is used by message at flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c in line 825.

	Source	Destination
File	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c	flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Line	832	861
Object	null	message

Code Snippet
File Name flatpak@@flatpak-1.15.9-CVE-2023-28101-TP.c
Method find_reverse_dep_apps (FlatpakTransaction *transaction,

```
....
832.    g_autoptr(GError) local_error = NULL;
....
861.                      flatpak_decomposed_get_ref (ref), local_error-
>message);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1453
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	866	827
Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
866.                      import = NULL;
....
827.                              &import->u.function, error_buf,
error_buf_size)) {
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1454
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	866	836

Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
866.                        import = NULL;
....
836.                                                field_name, &import-
>u.table,
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1455
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	866	848
Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
866.                        import = NULL;
....
848.                                                field_name, &import-
>u.memory,
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1456
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 693.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	866	858
Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
866.                        import = NULL;
....
858.                                                field_name, &import-
>u.global,
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1457
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 2371 is not initialized when it is used by Not at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 2297.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	2377	2305
Object	null	Not

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method load(const uint8 *buf, uint32 size, WASMModule *module, char *error_buf,

```
....
2377.       WASMSection *section_list = NULL;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method create_sections(const uint8 *buf, uint32 size, WASMSection **p_section_list,

```
....
2305.       bh_assert(!*p_section_list);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1458
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4717 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4721	3985
Object	null	dynamic_offset

Code Snippet

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4721.      uint8 *return_types = NULL;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3985.          ctx->dynamic_offset++;
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1459
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4625 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4630	3985
Object	null	dynamic_offset

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4630.       uint8 *types = NULL, *frame_ref;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3985.           ctx->dynamic_offset++;
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1460
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4625 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4630	3966
Object	null	dynamic_offset

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4630.       uint8 *types = NULL, *frame_ref;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3966.           emit_operand(ctx, ctx->dynamic_offset);
```

NULL Pointer Dereference\Path 22:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1461
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4717 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4721	3966
Object	null	dynamic_offset

Code Snippet

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4721.       uint8 *return_types = NULL;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3966.           emit_operand(ctx, ctx->dynamic_offset);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1462
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4625 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4630	3966
Object	null	dynamic_offset

Code Snippet

File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4630.       uint8 *types = NULL, *frame_ref;
```

File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3966.           emit_operand(ctx, ctx->dynamic_offset);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1463
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4717 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4721	3966
Object	null	dynamic_offset

Code Snippet

File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4721.       uint8 *return_types = NULL;
```

File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method	wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3966.           emit_operand(ctx, ctx->dynamic_offset);
```

NULL Pointer Dereference\Path 25:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1464
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4717 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4721	3968
Object	null	dynamic_offset

Code Snippet

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4721.      uint8 *return_types = NULL;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3968.          ctx->dynamic_offset++;
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1465
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4625 is not initialized when it is used by dynamic_offset at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3950.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4630	3968
Object	null	dynamic_offset

Code Snippet

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4630.       uint8 *types = NULL, *frame_ref;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3968.           ctx->dynamic_offset++;
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1466
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4717 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3344.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4721	3368
Object	null	frame_ref

Code Snippet

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4721.       uint8 *return_types = NULL;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3368.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1467

Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4625 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3344.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4630	3368
Object	null	frame_ref

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4630.       uint8 *types = NULL, *frame_ref;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3368.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1468
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4717 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3344.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4721	3362
Object	null	frame_ref

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4721.       uint8 *return_types = NULL;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3362.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1469
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 4625 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c in line 3344.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	4630	3362
Object	null	frame_ref

Code Snippet

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4630.       uint8 *types = NULL, *frame_ref;
```

File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c

Method wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3362.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1470
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c in line 1155 is not initialized when it is used by default_memory at fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c in line 1155.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	1314	1313
Object	null	default_memory

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Method wasm_instantiate(WASMModule *module, bool is_sub_inst, uint32 stack_size,

```
....
1314.          module_inst->memory_count ? module_inst->memories[0] :
NULL;
....
1313.      module_inst->default_memory =
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1471
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c in line 1155 is not initialized when it is used by default_table at fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c in line 1155.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Line	1399	1398
Object	null	default_table

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-48105-TP.c
Method wasm_instantiate(WASMModule *module, bool is_sub_inst, uint32 stack_size,

```
....
1399.          module_inst->table_count ? module_inst->tables[0] : NULL;
....
1398.      module_inst->default_table =
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1472
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	841	802
Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
841.                        import = NULL;
....
802.                                &import->u.function, error_buf,
error_buf_size)) {
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1473
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	841	811
Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
841.                        import = NULL;
....
811.                                                field_name, &import-
>u.table,
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1474
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	841	823
Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
841.                        import = NULL;
....
823.                                                field_name, &import-
>u.memory,
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1475
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668 is not initialized when it is used by u at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 668.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	841	833

Object	null	u

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load_import_section(const uint8 *buf, const uint8 *buf_end, WASMModule *module,

```
....
841.                        import = NULL;
....
833.                                                field_name, &import-
>u.global,
```

NULL Pointer Dereference\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1476
Status New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 2328 is not initialized when it is used by Not at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 2254.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	2334	2262
Object	null	Not

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method load(const uint8 *buf, uint32 size, WASMModule *module, char *error_buf,

```
....
2334.      WASMSection *section_list = NULL;
```

File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method create_sections(const uint8 *buf, uint32 size, WASMSection **p_section_list,

```
....
2262.      bh_assert(!*p_section_list);
```

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1477

Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4660 is not initialized when it is used by frame_offset at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3893.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4664	3926
Object	null	frame_offset

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4664.       uint8 *return_types = NULL;
```

File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3926.       ctx->frame_offset++;
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1478
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4568 is not initialized when it is used by frame_offset at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3893.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4573	3926
Object	null	frame_offset

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4573.       uint8 *types = NULL, *frame_ref;
```

File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	wasm_loader_push_frame_offset(WASMLoaderContext *ctx, uint8 type,

```
....
3926.       ctx->frame_offset++;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1479
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4660 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3297.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4664	3321
Object	null	frame_ref

Code Snippet

File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4664.       uint8 *return_types = NULL;
```

File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3321.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1480
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4568 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3297.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4573	3321
Object	null	frame_ref

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4573.       uint8 *types = NULL, *frame_ref;
```

File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c

Method wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3321.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1481
Status New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4660 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3297.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4664	3315
Object	null	frame_ref

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method check_block_stack(WASMLoaderContext *loader_ctx, BranchBlock *block,

```
....
4664.       uint8 *return_types = NULL;
```

File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c

Method	wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3315.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1482
Status	New

The variable declared in null at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 4568 is not initialized when it is used by frame_ref at fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c in line 3297.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	4573	3315
Object	null	frame_ref

Code Snippet

File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	wasm_loader_check_br(WASMLoaderContext *loader_ctx, uint32 depth,

```
....
4573.       uint8 *types = NULL, *frame_ref;
```

File Name	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method	wasm_loader_pop_frame_ref(WASMLoaderContext *ctx, uint8 type, char *error_buf,

```
....
3315.       ctx->frame_ref--;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1483
Status	New

The variable declared in null at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064 is not initialized when it is used by import_module at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	1128	1128
Object	null	import_module

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
1128.       function->import_module = is_native_symbol ? NULL :
sub_module;
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1484
Status New

The variable declared in null at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064 is not initialized when it is used by import_module at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	1075	1128
Object	null	import_module

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
1075.       WASMModule *sub_module = NULL;
....
1128.       function->import_module = is_native_symbol ? NULL :
sub_module;
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1485
Status New

The variable declared in null at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064 is not initialized when it is used by func_ptr_linked at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	1123	1123
Object	null	func_ptr_linked

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
1123.       function->func_ptr_linked = is_native_symbol ? linked_func :
NULL;
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1486
Status	New

The variable declared in null at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064 is not initialized when it is used by import_func_linked at fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c in line 1064.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	1129	1129
Object	null	import_func_linked

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
1129.       function->import_func_linked = is_native_symbol ? NULL :
linked_func;
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1487
Status	New

The variable declared in null at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 1064 is not initialized when it is used by import_module at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 1064.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	1128	1128
Object	null	import_module

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
1128.       function->import_module = is_native_symbol ? NULL :
sub_module;
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1488
Status	New

The variable declared in null at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 1064 is not initialized when it is used by import_module at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 1064.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	1075	1128
Object	null	import_module

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
1075.       WASMModule *sub_module = NULL;
....
1128.       function->import_module = is_native_symbol ? NULL :
sub_module;
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1489
Status	New

The variable declared in null at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 1064 is not initialized when it is used by func_ptr_linked at fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c in line 1064.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	1123	1123
Object	null	func_ptr_linked

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method load_function_import(const uint8 **p_buf, const uint8 *buf_end,

```
....
1123.       function->func_ptr_linked = is_native_symbol ? linked_func :
NULL;
```

Use of Obsolete Functions

Query Path:
CPP\Cx\CPP Low Visibility\Use of Obsolete Functions Version:0

Categories

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

Description
Use of Obsolete Functions\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1894
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1063	1063
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1063.       bcopy((uint8_t *) _private, private_key, num_bytes);
```

Use of Obsolete Functions\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1895
Status New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1064	1064
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1064.       bcopy((uint8_t *) _public, public_key, num_bytes*2);
```

Use of Obsolete Functions\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1896
Status New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1086	1086
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1086.       bcopy((uint8_t *) secret, (uint8_t *) _public, num_bytes);
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1897
Status	New

Method uECC_decompress in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1106, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1114	1114
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method void uECC_decompress(const uint8_t *compressed, uint8_t *public_key, uECC_Curve curve) {

```
....
1114.       bcopy(public_key, compressed+1, curve->num_bytes);
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1898
Status	New

Method bits2int in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1208, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1224	1224
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method static void bits2int(uECC_word_t *native,

```
....
1224.      bcopy((uint8_t *) native, bits, bits_size);
```

Use of Obsolete Functions\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1899
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1306	1306
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1306.      bcopy((uint8_t *) tmp, private_key, BITS_TO_BYTES(curve->num_n_bits));
```

Use of Obsolete Functions\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1900
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1322	1322
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1322.      bcopy((uint8_t *) signature + curve->num_bytes, (uint8_t *)
s, curve->num_bytes);
```

Use of Obsolete Functions\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1901
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1520	1520
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1520.      bcopy((uint8_t *) r, signature, curve->num_bytes);
```

Use of Obsolete Functions\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1902
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	1521	1521
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1521.      bcopy((uint8_t *) s, signature + curve->num_bytes, curve-
>num_bytes);
```

Use of Obsolete Functions\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1903
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1063	1063
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1063.      bcopy((uint8_t *) _private, private_key, num_bytes);
```

Use of Obsolete Functions\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1904
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1064	1064
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1064.       bcopy((uint8_t *) _public, public_key, num_bytes*2);
```

Use of Obsolete Functions\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1905
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1086	1086
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1086.       bcopy((uint8_t *) secret, (uint8_t *) _public, num_bytes);
```

Use of Obsolete Functions\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1906
Status	New

Method uECC_decompress in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1106, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1114	1114
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method void uECC_decompress(const uint8_t *compressed, uint8_t *public_key, uECC_Curve curve) {

```
....
1114.       bcopy(public_key, compressed+1, curve->num_bytes);
```

Use of Obsolete Functions\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1907
Status	New

Method bits2int in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1208, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1224	1224
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method static void bits2int(uECC_word_t *native,

```
....
1224.       bcopy((uint8_t *) native, bits, bits_size);
```

Use of Obsolete Functions\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1908
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1306	1306
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1306.      bcopy((uint8_t *) tmp, private_key, BITS_TO_BYTES(curve->num_n_bits));
```

Use of Obsolete Functions\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1909
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1322	1322
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1322.      bcopy((uint8_t *) signature + curve->num_bytes, (uint8_t *) s, curve->num_bytes);
```

Use of Obsolete Functions\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1910
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1520	1520
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1520.      bcopy((uint8_t *) r, signature, curve->num_bytes);
```

Use of Obsolete Functions\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1911
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	1521	1521
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1521.      bcopy((uint8_t *) s, signature + curve->num_bytes, curve-
>num_bytes);
```

Use of Obsolete Functions\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1912
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1063	1063
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1063.       bcopy((uint8_t *) _private, private_key, num_bytes);
```

Use of Obsolete Functions\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1913
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1064	1064
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1064.       bcopy((uint8_t *) _public, public_key, num_bytes*2);
```

Use of Obsolete Functions\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1914
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1086	1086
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1086.       bcopy((uint8_t *) secret, (uint8_t *) _public, num_bytes);
```

Use of Obsolete Functions\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1915
Status	New

Method uECC_decompress in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1106, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1114	1114
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method void uECC_decompress(const uint8_t *compressed, uint8_t *public_key, uECC_Curve curve) {

```
....
1114.       bcopy(public_key, compressed+1, curve->num_bytes);
```

Use of Obsolete Functions\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1916
Status	New

Method bits2int in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1208, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1224	1224
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method static void bits2int(uECC_word_t *native,

```
....
1224.      bcopy((uint8_t *) native, bits, bits_size);
```

Use of Obsolete Functions\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1917
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1306	1306
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1306.      bcopy((uint8_t *) tmp, private_key, BITS_TO_BYTES(curve->num_n_bits));
```

Use of Obsolete Functions\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1918
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1322	1322
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1322.      bcopy((uint8_t *) signature + curve->num_bytes, (uint8_t *)
s, curve->num_bytes);
```

Use of Obsolete Functions\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1919
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1520	1520
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1520.      bcopy((uint8_t *) r, signature, curve->num_bytes);
```

Use of Obsolete Functions\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1920
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	1521	1521
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1521.      bcopy((uint8_t *) s, signature + curve->num_bytes, curve-
>num_bytes);
```

Use of Obsolete Functions\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1921
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1063	1063
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1063.      bcopy((uint8_t *) _private, private_key, num_bytes);
```

Use of Obsolete Functions\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1922
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1064	1064
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1064.       bcopy((uint8_t *) _public, public_key, num_bytes*2);
```

Use of Obsolete Functions\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1923
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1086	1086
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1086.       bcopy((uint8_t *) secret, (uint8_t *) _public, num_bytes);
```

Use of Obsolete Functions\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1924
Status	New

Method uECC_decompress in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1106, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1114	1114
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method void uECC_decompress(const uint8_t *compressed, uint8_t *public_key, uECC_Curve curve) {

```
....
1114.      bcopy(public_key, compressed+1, curve->num_bytes);
```

Use of Obsolete Functions\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1925
Status	New

Method bits2int in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1208, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1224	1224
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method static void bits2int(uECC_word_t *native,

```
....
1224.      bcopy((uint8_t *) native, bits, bits_size);
```

Use of Obsolete Functions\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1926
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1306	1306
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1306.      bcopy((uint8_t *) tmp, private_key, BITS_TO_BYTES(curve->num_n_bits));
```

Use of Obsolete Functions\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1927
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1322	1322
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1322.      bcopy((uint8_t *) signature + curve->num_bytes, (uint8_t *) s, curve->num_bytes);
```

Use of Obsolete Functions\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1928
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1520	1520
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1520.      bcopy((uint8_t *) r, signature, curve->num_bytes);
```

Use of Obsolete Functions\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1929
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	1521	1521
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1521.      bcopy((uint8_t *) s, signature + curve->num_bytes, curve->num_bytes);
```

Use of Obsolete Functions\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1930
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1063	1063
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1063.       bcopy((uint8_t *) _private, private_key, num_bytes);
```

Use of Obsolete Functions\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1931
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1064	1064
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1064.       bcopy((uint8_t *) _public, public_key, num_bytes*2);
```

Use of Obsolete Functions\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1932
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1086	1086
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1086.       bcopy((uint8_t *) secret, (uint8_t *) _public, num_bytes);
```

Use of Obsolete Functions\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1933
Status	New

Method uECC_decompress in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1106, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1114	1114
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method void uECC_decompress(const uint8_t *compressed, uint8_t *public_key, uECC_Curve curve) {

```
....
1114.       bcopy(public_key, compressed+1, curve->num_bytes);
```

Use of Obsolete Functions\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1934
Status	New

Method bits2int in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1208, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1224	1224
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method static void bits2int(uECC_word_t *native,

```
....
1224.      bcopy((uint8_t *) native, bits, bits_size);
```

Use of Obsolete Functions\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1935
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1306	1306
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1306.      bcopy((uint8_t *) tmp, private_key, BITS_TO_BYTES(curve->num_n_bits));
```

Use of Obsolete Functions\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1936
Status	New

Method uECC_sign_with_k_internal in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1246, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1322	1322
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method static int uECC_sign_with_k_internal(const uint8_t *private_key,

```
....
1322.      bcopy((uint8_t *) signature + curve->num_bytes, (uint8_t *)
s, curve->num_bytes);
```

Use of Obsolete Functions\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1937
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1520	1520
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1520.      bcopy((uint8_t *) r, signature, curve->num_bytes);
```

Use of Obsolete Functions\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1938
Status	New

Method uECC_verify in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c, at line 1489, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	1521	1521
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1521.      bcopy((uint8_t *) s, signature + curve->num_bytes, curve-
>num_bytes);
```

Use of Obsolete Functions\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1939
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	1063	1063
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1063.      bcopy((uint8_t *) _private, private_key, num_bytes);
```

Use of Obsolete Functions\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1940
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	1064	1064
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1064.       bcopy((uint8_t *) _public, public_key, num_bytes*2);
```

Use of Obsolete Functions\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1941
Status	New

Method uECC_shared_secret in flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c, at line 1048, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	1086	1086
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method int uECC_shared_secret(const uint8_t *public_key,

```
....
1086.       bcopy((uint8_t *) secret, (uint8_t *) _public, num_bytes);
```

Use of Obsolete Functions\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1942
Status	New

Method uECC_decompress in flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c, at line 1106, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	1114	1114
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method void uECC_decompress(const uint8_t *compressed, uint8_t *public_key, uECC_Curve curve) {

```
....
1114.       bcopy(public_key, compressed+1, curve->num_bytes);
```

Use of Obsolete Functions\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1943
Status	New

Method bits2int in flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c, at line 1208, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	1224	1224
Object	bcopy	bcopy

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method static void bits2int(uECC_word_t *native,

```
....
1224.       bcopy((uint8_t *) native, bits, bits_size);
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1413
Status	New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-	flipperdevices@@flipperzero-firmware-

	0.44.1-CVE-2021-3520-FP.c	0.44.1-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.          for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1414
Status	New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.          for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1415
Status	New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.            for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1416
Status	New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.            for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1417
Status	New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.            for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1418
Status	New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.            for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1419
Status	New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.            for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1420
Status New

The buffer allocated by <= in flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.            for (i = 0; i <= k; ++i) {
```

Potential Off by One Error in Loops\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1421
Status New

The buffer allocated by <= in fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c at line 3026 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Line	3279	3279
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3279.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1422
Status New

The buffer allocated by <= in fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c at line 3026 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Line	3279	3279
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v1.8.12-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3279.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1423
Status New

The buffer allocated by <= in fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c at line 3026 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Line	3279	3279
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3279.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1424
Status New

The buffer allocated by <= in fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c at line 3026 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Line	3279	3279
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v1.9.3-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3279.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1425
Status New

The buffer allocated by <= in fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c at line 3026 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c	fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Line	3279	3279
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v1.9.7-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3279.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1426
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c at line 3028 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Line	3284	3284
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3284.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1427
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c at line 4913 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	5297	5297
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
5297.                   for (i = 0; i <= count; i++) {
```

Potential Off by One Error in Loops\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1428
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c at line 2533 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Line	2655	2655
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-52284-TP.c
Method wasm_loader_find_block_addr(WASMExecEnv *exec_env, BlockAddr *block_addr_cache,

```
....
2655.                   for (i = 0; i <= count; i++) /* lableidxs */
```

Potential Off by One Error in Loops\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1429
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c at line 3028 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Line	3284	3284
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3284.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1430
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c at line 4856 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	5244	5244
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
5244.                   for (i = 0; i <= count; i++) {
```

Potential Off by One Error in Loops\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1431
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c at line 2490 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Line	2612	2612
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.0.5-CVE-2023-52284-TP.c
Method wasm_loader_find_block_addr(WASMExecEnv *exec_env, BlockAddr *block_addr_cache,

```
....
2612.                   for (i = 0; i <= count; i++) /* lableidxs */
```

Potential Off by One Error in Loops\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1432
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c at line 3028 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Line	3284	3284
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3284.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1433
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c at line 7197 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	7599	7599
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
7599.                   for (i = 0; i <= count; i++) {
```

Potential Off by One Error in Loops\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1434
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c at line 4454 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Line	4578	4578
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-48105-TP.c
Method wasm_loader_find_block_addr(WASMExecEnv *exec_env, BlockAddr *block_addr_cache,

```
....
4578.                   for (i = 0; i <= count; i++) /* lableidxs */
```

Potential Off by One Error in Loops\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1435
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c at line 7197 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	7599	7599
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method wasm_loader_prepare_bytecode(WASMModule *module, WASMFunction *func,

```
....
7599.                   for (i = 0; i <= count; i++) {
```

Potential Off by One Error in Loops\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1436
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c at line 4454 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c	fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Line	4578	4578
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.1.9-CVE-2023-52284-TP.c
Method wasm_loader_find_block_addr(WASMExecEnv *exec_env, BlockAddr *block_addr_cache,

```
....
4578.                   for (i = 0; i <= count; i++) /* lableidxs */
```

Potential Off by One Error in Loops\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1437
Status New

The buffer allocated by <= in fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c at line 3028 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Line	3284	3284
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v2.2.1-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3284.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1438
Status New

The buffer allocated by <= in fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c at line 3028 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Line	3284	3284
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3284.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1439
Status New

The buffer allocated by <= in fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c at line 3026 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c	fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Line	3279	3279
Object	<=	<=

Code Snippet
File Name fluent@@fluent-bit-v3.1.0-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3279.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1537
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	434	434
Object	data	sizeof

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_write_block(PicopassBlock* AA1, uint8_t blockNo, uint8_t* newBlock) {

```
....
434.      loclass_doMAC_N(data, sizeof(data),
AA1[PICOPASS_KD_BLOCK_INDEX].data, mac);
```

Sizeof Pointer Argument\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1538
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Line	381	381
Object	data	sizeof

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_write_card(PicopassBlock* AA1) {

```
....
381.          loclass_doMAC_N(data, sizeof(data), div_key, mac);
```

Sizeof Pointer Argument\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1539
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Line	353	353
Object	data	sizeof

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2022-38890-FP.c
Method ReturnCode picopass_write_card(PicopassBlock* AA1) {

```
....
353.          loclass_doMAC_N(data, sizeof(data), div_key, mac);
```

Sizeof Pointer Argument\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1540
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	378	378

Object	dir_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
378.                if (dir_list_size >= sizeof(dir_list) / sizeof(char
*)) {
```

Sizeof Pointer Argument\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1541
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	390	390
Object	env_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
390.                if (env_list_size >= sizeof(env_list) / sizeof(char
*)) {
```

Sizeof Pointer Argument\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1542
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	429	429
Object	ns_lookup_pool	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c

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

```
....
429.                    >= sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])) {
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1543
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	429	429
Object	ns_lookup_pool	sizeof

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method	main(int argc, char *argv[])

```
....
429.                    >= sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])) {
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1544
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	415	415
Object	addr_pool	sizeof

Code Snippet	
File Name	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method	main(int argc, char *argv[])

```
....
415.                    if (addr_pool_size >= sizeof(addr_pool) /
sizeof(char *)) {
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1545
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	442	442
Object	native_lib_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
442.                if (native_lib_count >= sizeof(native_lib_list) /
sizeof(char *)) {
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1546
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	380	380
Object	dir_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
380.                            (int)(sizeof(dir_list) / sizeof(char *)));
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1547
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	378	380
Object	dir_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
378.              if (dir_list_size >= sizeof(dir_list) / sizeof(char
*)) {
....
380.                          (int)(sizeof(dir_list) / sizeof(char *)));
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1548
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	392	392
Object	env_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
392.                          (int)(sizeof(env_list) / sizeof(char *)));
```

Sizeof Pointer Argument\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1549
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	390	392
Object	env_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
390.              if (env_list_size >= sizeof(env_list) / sizeof(char
*)) {
....
392.                          (int)(sizeof(env_list) / sizeof(char *)));
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1550
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	432	432
Object	ns_lookup_pool	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
432.                        (int)(sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])));
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1551
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	429	432
Object	ns_lookup_pool	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
429.                    >= sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])) {
....
432.                        (int)(sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])));
```

Sizeof Pointer Argument\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1552
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	432	432
Object	ns_lookup_pool	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
432.                        (int)(sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])));
```

Sizeof Pointer Argument\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1553
Status New

	Source	Destination

File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	429	432
Object	ns_lookup_pool	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
429.                    >= sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])) {
....
432.                        (int)(sizeof(ns_lookup_pool) /
sizeof(ns_lookup_pool[0])));
```

Sizeof Pointer Argument\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1554
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	417	417
Object	addr_pool	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
417.                                (int)(sizeof(addr_pool) / sizeof(char
*)));
```

Sizeof Pointer Argument\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1555
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c

Line	415	417
Object	addr_pool	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
415.                    if (addr_pool_size >= sizeof(addr_pool) /
sizeof(char *)) {
....
417.                                (int)(sizeof(addr_pool) / sizeof(char
*)));
```

Sizeof Pointer Argument\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1556
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	444	444
Object	native_lib_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
444.                           (int)(sizeof(native_lib_list) / sizeof(char
*)));
```

Sizeof Pointer Argument\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1557
Status New

	Source	Destination
File	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c	fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Line	442	444

Object	native_lib_list	sizeof

Code Snippet
File Name fluent@@fluent-bit-v2.0.14-CVE-2023-48105-TP.c
Method main(int argc, char *argv[])

```
....
442.              if (native_lib_count >= sizeof(native_lib_list) /
sizeof(char *)) {
....
444.                          (int)(sizeof(native_lib_list) / sizeof(char
*)));
```

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=1000023&projectid=13&pathid=1521
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1522
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.44.1-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1523
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1524
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Line	484	484

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1525
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1526
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1527
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1528
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1529
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1530
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1531
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1532
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1533
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c
Line	402	402

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1534
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1535
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c
Method static void muladd(uECC_word_t a,

```
....
402.      *r1 += (p1 + (*r0 < p0));
```

Arithmenic Operation On Boolean\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1536
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-3520-FP.c
Method static void mul2add(uECC_word_t a,

```
....
484.      *r1 += (p1 + (*r0 < p0));
```

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=1000023&projectid=13&pathid=1966
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c
Line	276	276
Object	str_loc	str_loc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.103.0-rc-CVE-2021-32020-FP.c

Method	char* ultoa(unsigned long num, char* str, int radix) {

```
....
276.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1967
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Line	330	330
Object	position	position

Code Snippet	
File Name	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Method	static void byte_input_set_nibble(uint8_t* data, uint8_t position, char value, bool high_nibble) {

```
....
330.          data[position] &= 0x0F;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1968
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Line	331	331
Object	position	position

Code Snippet	
File Name	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Method	static void byte_input_set_nibble(uint8_t* data, uint8_t position, char value, bool high_nibble) {

```
....
331.          data[position] |= value << 4;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1969
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Line	333	333
Object	position	position

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Method static void byte_input_set_nibble(uint8_t* data, uint8_t position, char value, bool high_nibble) {

```
....
333.            data[position] &= 0xF0;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1970
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c	flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Line	334	334
Object	position	position

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.31.2-CVE-2021-3520-FP.c
Method static void byte_input_set_nibble(uint8_t* data, uint8_t position, char value, bool high_nibble) {

```
....
334.            data[position] |= value;
```

Unchecked Array Index\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1971
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Line	266	266
Object	str_loc	str_loc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.52.3-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
266.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1972
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Line	276	276
Object	str_loc	str_loc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.62.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
276.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1973
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-	flipperdevices@@flipperzero-firmware-

	0.69.0-rc-CVE-2021-32020-FP.c	0.69.0-rc-CVE-2021-32020-FP.c
Line	275	275
Object	str_loc	str_loc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.69.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
275.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1974
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Line	276	276
Object	str_loc	str_loc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.76.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
276.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1975
Status New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Line	276	276
Object	str_loc	str_loc

Code Snippet

File Name	flipperdevices@@flipperzero-firmware-0.83.0-rc-CVE-2021-32020-TP.c
Method	char* ultoa(unsigned long num, char* str, int radix) {

```
....
276.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1976
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Line	276	276
Object	str_loc	str_loc

Code Snippet

File Name	flipperdevices@@flipperzero-firmware-0.89.0-CVE-2021-32020-FP.c
Method	char* ultoa(unsigned long num, char* str, int radix) {

```
....
276.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1977
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Line	277	277
Object	str_loc	str_loc

Code Snippet

File Name	flipperdevices@@flipperzero-firmware-0.95.0-CVE-2021-32020-FP.c
Method	char* ultoa(unsigned long num, char* str, int radix) {

```
....
277.      str[str_loc] = 0; // add null termination.
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1978
Status	New

	Source	Destination
File	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c	flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Line	281	281
Object	str_loc	str_loc

Code Snippet
File Name flipperdevices@@flipperzero-firmware-0.99.0-rc-CVE-2021-32020-FP.c
Method char* ultoa(unsigned long num, char* str, int radix) {

```
....
281.      str[str_loc] = 0; // add null termination.
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1571
Status	New

The system data read by rconf_meta_add in the file fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c at line 43 is potentially exposed by rconf_meta_add found in fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c at line 43.

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Line	56	56
Object	perror	perror

Code Snippet
File Name fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c

Method	static int rconf_meta_add(struct mk_rconf *conf, char *buf, int len)

```
....
56.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1572
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Line	170	170
Object	perror	perror

Code Snippet	
File Name	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Method	static int flb_config_static_read(struct mk_rconf *conf,

```
....
170.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1573
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Line	335	335
Object	perror	perror

Code Snippet

File Name	fluent@@fluent-bit-tiger-1.8.15-20230223-CVE-2024-4323-TP.c
Method	static int flb_config_static_read(struct mk_rconf *conf,

```
....
335.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1574
Status	New

The system data read by rconf_meta_add in the file fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c at line 43 is potentially exposed by rconf_meta_add found in fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c at line 43.

	Source	Destination
File	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Line	56	56
Object	perror	perror

Code Snippet	
File Name	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Method	static int rconf_meta_add(struct mk_rconf *conf, char *buf, int len)

```
....
56.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1575
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Line	170	170
Object	perror	perror

Code Snippet	
File Name	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Method	static int flb_config_static_read(struct mk_rconf *conf,

```
....
170.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1576
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Line	335	335
Object	perror	perror

Code Snippet	
File Name	fluent@@fluent-bit-v1.7.9-CVE-2024-4323-FP.c
Method	static int flb_config_static_read(struct mk_rconf *conf,

```
....
335.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1577
Status	New

The system data read by rconf_meta_add in the file fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c at line 43 is potentially exposed by rconf_meta_add found in fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c at line 43.

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Line	56	56
Object	perror	perror

Code Snippet	
File Name	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Method	static int rconf_meta_add(struct mk_rconf *conf, char *buf, int len)

```
....
56.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1578
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Line	170	170
Object	perror	perror

Code Snippet	
File Name	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Method	static int flb_config_static_read(struct mk_rconf *conf,

```
....
170.          perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1579
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Line	335	335

Object	perror	perror

Code Snippet
File Name fluent@@fluent-bit-v1.8.12-CVE-2024-4323-FP.c
Method static int flb_config_static_read(struct mk_rconf *conf,

```
....
335.           perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1580
Status	New

The system data read by rconf_meta_add in the file fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c at line 43 is potentially exposed by rconf_meta_add found in fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c at line 43.

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Line	56	56
Object	perror	perror

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Method static int rconf_meta_add(struct mk_rconf *conf, char *buf, int len)

```
....
56.           perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1581
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c

Line	170	170
Object	perror	perror

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Method static int flb_config_static_read(struct mk_rconf *conf,

```
....
170.            perror("malloc");
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1582
Status	New

The system data read by flb_config_static_read in the file fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c at line 141 is potentially exposed by flb_config_static_read found in fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c at line 141.

	Source	Destination
File	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c	fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Line	335	335
Object	perror	perror

Code Snippet
File Name fluent@@fluent-bit-v1.8.8-CVE-2024-4323-FP.c
Method static int flb_config_static_read(struct mk_rconf *conf,

```
....
335.            perror("malloc");
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13

	&pathid=1562
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c
Line	58	58
Object	fgets	fgets

Code Snippet
File Name fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c
Method ares_status_t ares__read_line(FILE *fp, char **buf, size_t *bufsize)

```
....
58.      if (!fgets(*buf + offset, bytestoread, fp)) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1563
Status	New

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c
Line	58	58
Object	fgets	fgets

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c
Method ares_status_t ares__read_line(FILE *fp, char **buf, size_t *bufsize)

```
....
58.      if (!fgets(*buf + offset, bytestoread, fp)) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1564
Status	New

	Source	Destination
File	fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c	fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c

Line	58	58
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name fluent@@fluent-bit-v2.2.1-CVE-2024-25629-TP.c
Method ares_status_t ares__read_line(FILE *fp, char **buf, size_t *bufsize)

```
....
58.      if (!fgets(*buf + offset, bytestoread, fp)) {
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1565
Status New

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c
Line	58	58
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2024-25629-TP.c
Method ares_status_t ares__read_line(FILE *fp, char **buf, size_t *bufsize)

```
....
58.      if (!fgets(*buf + offset, bytestoread, fp)) {
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1566
Status New

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c
Line	6896	6896
Object	fprintf	fprintf

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c

Method	ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6896.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1567
Status	New

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c
Line	6898	6898
Object	fprintf	fprintf

Code Snippet	
File Name	fluent@@fluent-bit-v3.0.1-CVE-2024-28182-TP.c
Method	ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6898.           fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1568
Status	New

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c
Line	6896	6896
Object	fprintf	fprintf

Code Snippet	
File Name	fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c
Method	ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6896.           fprintf(stderr, "recv: [IB_EXPECT_CONTINUATION]\n");
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1569
Status	New

	Source	Destination
File	fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c	fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c
Line	6898	6898
Object	fprintf	fprintf

Code Snippet
File Name fluent@@fluent-bit-v3.0.1-CVE-2024-4323-TP.c
Method ssize_t nghttp2_session_mem_recv(nghttp2_session *session, const uint8_t *in,

```
....
6898.          fprintf(stderr, "recv: [IB_IGN_CONTINUATION]\n");
```

Information Exposure Through Comments

Query Path:
CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description
Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1583
Status	New

	Source	Destination
File	flatpak@@flatpak-1.10.2-CVE-2021-43860-TP.c	flatpak@@flatpak-1.10.2-CVE-2021-43860-TP.c
Line	3460	3460
Object	password:	password:

Code Snippet
File Name flatpak@@flatpak-1.10.2-CVE-2021-43860-TP.c
Method * @password: The password

```
....
3460.    * @password: The password
```

Information Exposure Through Comments\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1584
Status	New

	Source	Destination
File	flatpak@@flatpak-1.10.4-CVE-2021-43860-TP.c	flatpak@@flatpak-1.10.4-CVE-2021-43860-TP.c
Line	3460	3460
Object	password:	password:

Code Snippet
File Name flatpak@@flatpak-1.10.4-CVE-2021-43860-TP.c
Method * @password: The password

```
....
3460.    * @password: The password
```

Information Exposure Through Comments\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1585
Status	New

	Source	Destination
File	flatpak@@flatpak-1.11.2-CVE-2021-43860-TP.c	flatpak@@flatpak-1.11.2-CVE-2021-43860-TP.c
Line	3479	3479
Object	password:	password:

Code Snippet
File Name flatpak@@flatpak-1.11.2-CVE-2021-43860-TP.c
Method * @password: The password

```
....
3479.    * @password: The password
```

Information Exposure Through Comments\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1586

Status	New

	Source	Destination
File	flatpak@@flatpak-1.6.3-CVE-2021-43860-TP.c	flatpak@@flatpak-1.6.3-CVE-2021-43860-TP.c
Line	2981	2981
Object	password:	password:

Code Snippet
File Name flatpak@@flatpak-1.6.3-CVE-2021-43860-TP.c
Method * @password: The password

```
....
2981.    * @password: The password
```

Information Exposure Through Comments\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1587
Status	New

	Source	Destination
File	flatpak@@flatpak-1.6.5-CVE-2021-43860-TP.c	flatpak@@flatpak-1.6.5-CVE-2021-43860-TP.c
Line	2981	2981
Object	password:	password:

Code Snippet
File Name flatpak@@flatpak-1.6.5-CVE-2021-43860-TP.c
Method * @password: The password

```
....
2981.    * @password: The password
```

Information Exposure Through Comments\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1588
Status	New

	Source	Destination
File	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41859-TP.c	FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41859-TP.c

Line	203	203
Object	pwd-	pwd-

Code Snippet
File Name FreeRADIUS@@freeradius-server-release_3_0_21-CVE-2022-41859-TP.c
Method * pwd-seed = H(token | peer-id | server-id | password |

```
....
203.                *     pwd-seed = H(token | peer-id | server-id |
password |
```

Information Exposure Through Comments\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1589
Status New

	Source	Destination
File	FreeRADIUS@@freeradius-server-release_3_0_22-CVE-2022-41859-TP.c	FreeRADIUS@@freeradius-server-release_3_0_22-CVE-2022-41859-TP.c
Line	360	360
Object	pwd-	pwd-

Code Snippet
File Name FreeRADIUS@@freeradius-server-release_3_0_22-CVE-2022-41859-TP.c
Method * pwd-seed = H(token | peer-id | server-id | password |

```
....
360.                *     pwd-seed = H(token | peer-id | server-id |
password |
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Incorrect Permission Assignment For Critical Resources\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000023&projectid=13&pathid=1570
Status New

	Source	Destination
File	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c	FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Line	176	176
Object	CreateFile	CreateFile

Code Snippet
File Name FreeRDP@@FreeRDP-2.0.0-CVE-2020-11089-TP.c
Method static UINT serial_process_irp_create(SERIAL_DEVICE* serial, IRP* irp)

```
....
176.            CreateFile(serial->device.name, DesiredAccess,
SharedAccess, NULL, /* SecurityAttributes */
```

Buffer Overflow cpycat

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 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

Process Control

Risk

What might happen

An attacker could:

- Change the command that the program executes or change the environment in which the command executes.
- Execute code contained in the native libraries, which often contain calls that are susceptible to other security problems, such as buffer overflows or command injection.
- Affect program parameters, which are part of execution environment, and/or affect the execution flow

Please note that if the application runs with elevated privileges, the content of the attacker's library will now be run with elevated privileges, possibly giving them complete control of the system.

Cause

How does it happen

Process control vulnerabilities occur when data enters the application from an untrusted source and is later used as, or as part of, a string representing a command that is executed in the application, using the Load-Library method. By controlling the name or path of the loaded library, an attacker can load and execute a malicious library instead of the intended one. This may lead to executing malicious commands (and payloads) on behalf of an attacker.

General Recommendations

How to avoid it

- Libraries that are loaded should come from a trusted source. If the library does not come from a trusted source, review its source code.
- All native libraries should be validated to determine if the application requires the use of the library.
- Run the application with the least-privilege principle in order to reduce the impact in case of a successful attack.

Secure-Code Approach

- Sanitize all inputs which influence the library calls in order to avoid malicious content.
- Use absolute path when calling the library in order to avoid calls to unwanted libraries.
- Validate all inputs to native calls in order to avoid buffer overflows.
- Use System.load, instead of System.loadLibrary, which is more secured.

Source Code Examples

CPP

Using an invalidated registry entry to determine the directory in which it is installed and loads a library file, allowing an attacker to load an arbitrary library:

```
RegQueryValueEx(hkey, "APPHOME", 0, 0, (BYTE*)home, &size);
char* lib=(char*)malloc(strlen(home)+strlen(INITLIB));
if (lib) {
    strcpy(lib,home);
    strcat(lib,INITCMD);
    LoadLibrary(lib);
}
```

Loading the library from its absolute path:

```
std::string apphome =
"HKEY_LOCAL_MACHINE\\SOFTWARE\MICROSOFT\\WINDOWS NT\\CurrentVersion\\ProfileList\\Default\\";
RegQueryValueEx(hkey, apphone, 0, 0, (BYTE*)home, &size);
char* lib=(char*)malloc(strlen(home)+strlen(INITLIB));
if (lib) {
    strcpy(lib,home);
    strcat(lib,INITCMD);
    LoadLibrary(lib);
}
```

CSharp

Using the application configuration property to load a native library, allowing an attacker to load a library or an executable and potentially execute arbitrary code:

```
string lib = ConfigurationManager.AppSettings["APPHOME"];
Environment.ExitCode = AppDomain.CurrentDomain.ExecuteAssembly(lib);
```

Validating the configuration property before loading a native library:

```
string lib = ConfigurationManager.AppSettings["APPHOME"];
if ( isValidHomePath(lib) )
{
    Environment.ExitCode = AppDomain.CurrentDomain.ExecuteAssembly(lib);
}
else
{
    Console.WriteLine("Action denied.");
}
```

Java

Loading a library from the default Java library path, without validating it:

```
System.loadLibrary("crypto.so");
```

Using an invalidated system property to determine the directory in which it is installed and loads a library file, allowing an attacker to load an arbitrary library:

```
String property = System.getProperty("java.library.path");
System.loadLibrary(property);
```

Loading the library from its absolute path using System.load:

```
String path = "/path/to/lib/";
String lib = "crypto.so";
System.load(path + lib);
```

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

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;
}
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

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

Download of Code Without Integrity Check

Risk

What might happen

At best, code that fails an integrity check may be damaged, altered or may not match the intended code that it originally was, resulting in unexpected behavior. At worst, attackers who are able to compromise the loaded code, such as locally or via a Man-in-the-Middle attack, may alter the loaded code either at storage or in transit, which may result in malicious code execution and significant system compromise.

Cause

How does it happen

Integrity signatures, as derived from any data set, can allow a recepient to identify that the received data set is the one they intended to obtain. For externally loaded code this is particularly important, as such code can be compromised via access to local storage, Man-in-the-Middle attacks and more.

General Recommendations

How to avoid it

Perform strict integrity checks to ensure code obtained from external sources is verified, and has a known and trusted signature.

Source Code Examples

Java

Calculate Hash of File And Compare to Trusted Hash

```
byte[] dataBytes = new byte[1024];
MessageDigest md = MessageDigest.getInstance("SHA-256");
int nread = 0;

//Create byte hash from file
FileInputStream fis = new FileInputStream(file);
while ((nread = fis.read(dataBytes)) != -1) {
      md.update(dataBytes, 0, nread);
};
fis.close();

//Convert bytes to hex
byte[] mdbytes = md.digest();
StringBuffer sb = new StringBuffer();
for (int i = 0; i < mdbytes.length; i++) {
      sb.append(Integer.toString((mdbytes[i] & 0xff) + 0x100, 16).substring(1));
}
String sha256ofFile = sb.toString();

if (sha256ofFile.equals(TRUSTED_SHA256_OF_FILE)) {
      // Handle trusted files here
}
else {
      // Handle untrusted files here
}
```

Class Function Loaded From Untested External File

```
private void LoadClass (File file) {
      URL url = file.toURI().toURL();
      URL[] urls = new URL[]{url};
      ClassLoader cl = new URLClassLoader(urls);
      Class cls = cl.loadClass("com.packagename.classname");
      Constructor cons = cls.getConstructor();
      Object simpleClassObj = cons.newInstance();
      Method method = cls.getMethod("functionname");
      method.invoke(simpleClassObj);
}
```

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Wrong Memory Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
```

```
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Stored Buffer Overflow fgets

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));
    }
}
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

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

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

Information Leak Through Comments

Weakness ID: 615 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

- Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

Reference	Description
CVE-2007-6197	Version numbers and internal hostnames leaked in HTML comments.
CVE-2007-4072	CMS places full pathname of server in HTML comment.
CVE-2009-2431	blog software leaks real username in HTML comment.

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	**Development Concepts (primary)699 Research Concepts (primary)1000**

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	Anonymous Tool Vendor (under NDA)		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal

	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

BACK TO TOP

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

Use of Obsolete Functions

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

Java

Using Deprecated Methods for Security Checks

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        secManager.checkMulticast(address, 0)
    }

}
```

A Replacement Security Check

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        SocketPermission permission = new SocketPermission(address.getHostAddress(),
"accept,connect");

        secManager.checkPermission(permission)
    }
```

```
}
```

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