vul_files_29 Scan Report

Project Name	vul_files_29
Scan Start	Tuesday, January 7, 2025 3:11:05 PM
Preset	Checkmarx Default
Scan Time	03h:31m:38s
Lines Of Code Scanned	299402
Files Scanned	205
Report Creation Time	Tuesday, January 7, 2025 6:17:20 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

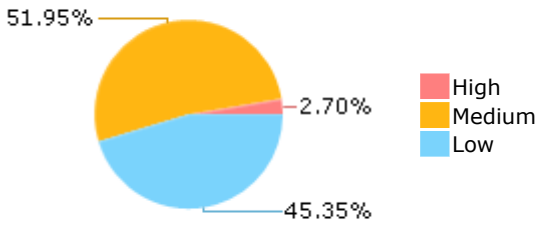
Results Limit

Results limit per query was set to 50

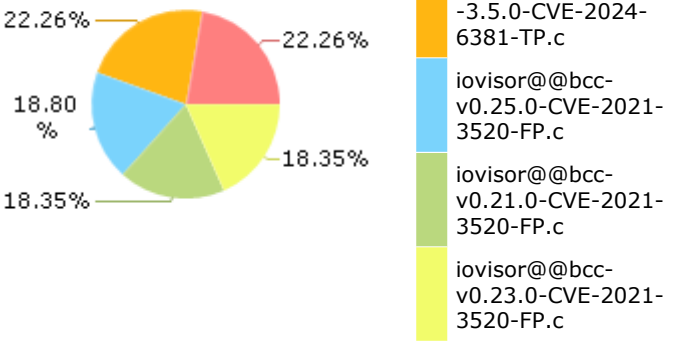
Selected Queries

Selected queries are listed in Result Summary

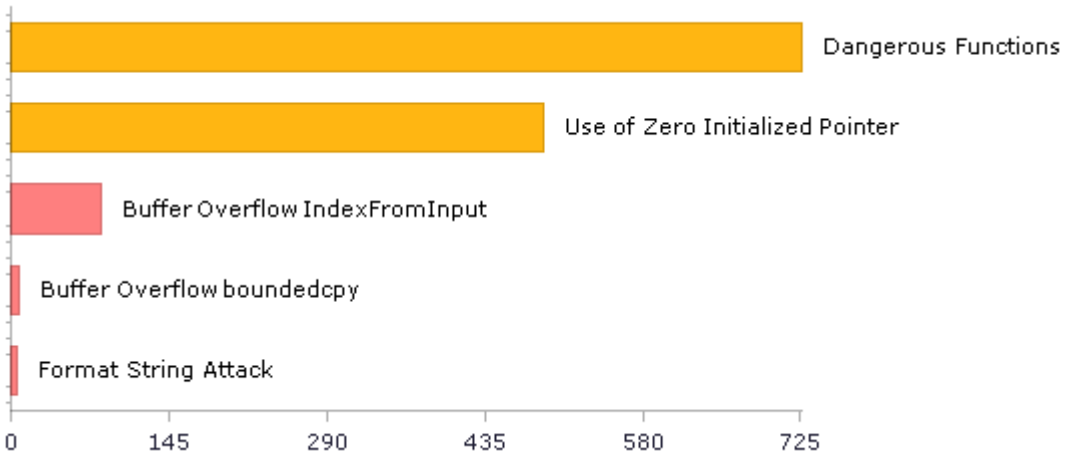
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	768	564
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	862	862
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	75	20
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	2	2
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	735	735
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	2	2
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	75	20
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	735	735
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	6	6
PCI DSS (3.2) - 6.5.2 - Buffer overflows	375	360
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.	48	48
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.	11	11
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.	32	7
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.	814	814
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.	75	20
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	6	6

***** 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)	894	869
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)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	949	556
SC-8 Transmission Confidentiality and Integrity (P1)	75	20
SI-10 Information Input Validation (P1)*	115	87
SI-11 Error Handling (P2)*	126	126
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	13	13

***** 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

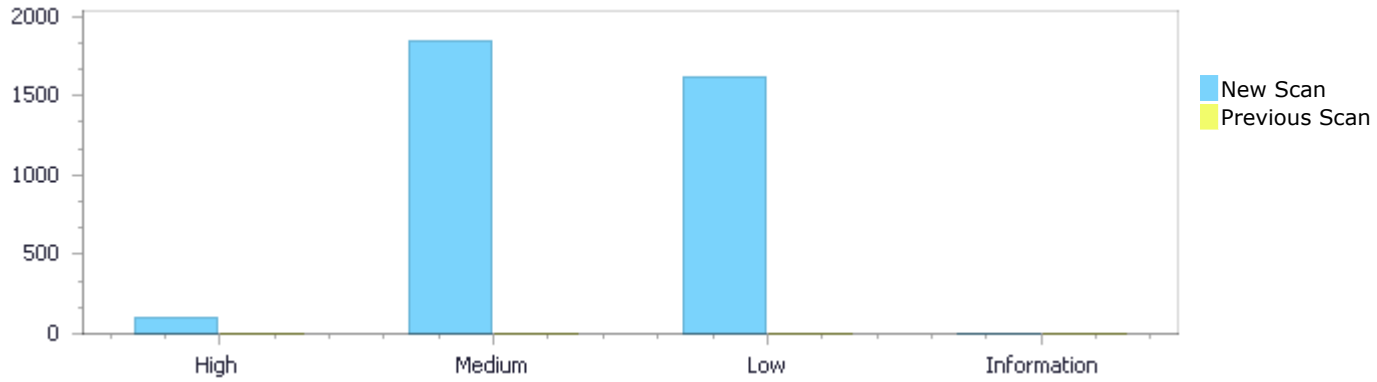
Scan Summary - Custom

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	96	1,848	1,613	0	3,557
Recurrent Issues	0	0	0	0	0
Total	96	1,848	1,613	0	3,557
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	96	1,848	1,613	0	3,557
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	96	1,848	1,613	0	3,557

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	83	High
Buffer Overflow boundedcpy	8	High
Format String Attack	5	High
Dangerous Functions	726	Medium
Use of Zero Initialized Pointer	488	Medium

Buffer Overflow boundcpy WrongSizeParam	320	Medium
Memory Leak	116	Medium
MemoryFree on StackVariable	80	Medium
Wrong Size t Allocation	47	Medium
Divide By Zero	22	Medium
Stored Buffer Overflow boundcpy	21	Medium
Buffer Overflow AddressOfLocalVarReturned	10	Medium
Double Free	7	Medium
Integer Overflow	6	Medium
Use of Uninitialized Variable	4	Medium
Use of Uninitialized Pointer	1	Medium
Improper Resource Access Authorization	814	Low
NULL Pointer Dereference	261	Low
Unchecked Return Value	126	Low
Insufficiently Protected Credentials	75	Low
Unreleased Resource Leak	58	Low
TOCTOU	50	Low
Incorrect Permission Assignment For Critical Resources	48	Low
Use of Sizeof On a Pointer Type	45	Low
Exposure of System Data to Unauthorized Control Sphere	32	Low
Potential Precision Problem	28	Low
Heuristic 2nd Order Buffer Overflow malloc	23	Low
Unchecked Array Index	21	Low
Arithmenic Operation On Boolean	11	Low
Use of Obsolete Functions	9	Low
Potential Off by One Error in Loops	6	Low
Heuristic Buffer Overflow malloc	3	Low
Potential Path Traversal	2	Low
Inconsistent Implementations	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	75
jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	75
iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	57
iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	57
iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	57
krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	52
krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	52
krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	52
krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	52
krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c	52

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=14
Status	New

The size of the buffer used by main in optind, at line 38 of krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.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 argc, at line 38 of krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.c
Line	38	69
Object	argc	optind

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.c
Method main(int argc, char **argv)

```
....
38.  main(int argc, char **argv)
....
69.      ret = krb5_parse_name(context, argv[optind], &princ);
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=15
Status	New

The size of the buffer used by *ksyms__load in i, at line 98 of iovisor@@bcc-0.29.0-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 *ksyms__load passes to f, at line 98 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination

File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	115	127
Object	f	i

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
115.              ret = fscanf(f, "%lx %c %s%*[^\n]\n",
....
127.              ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=16
Status New

The size of the buffer used by *ksyms__load in i, at line 98 of iovisor@@bcc-0.29.0-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 *ksyms__load passes to sym_name, at line 98 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	116	127
Object	sym_name	i

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
116.                          &sym_addr, &sym_type, sym_name);
....
127.              ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=17
Status New

The size of the buffer used by syms__add_dso in i, at line 323 of iovisor@@bcc-0.29.0-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 *syms__load_file passes to buf, at line 656 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	680	330
Object	buf	i

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
680.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
330.                if (!strcmp(syms->dsos[i].name, name)) {
```

Buffer Overflow IndexFromInput\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=18
Status New

The size of the buffer used by *syms_cache__get_syms in nr, at line 789 of iovisor@@bcc-0.29.0-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 *syms__load_file passes to buf, at line 656 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	680	804
Object	buf	nr

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
680.                          (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method struct syms *syms_cache__get_syms(struct syms_cache *syms_cache, int tgid)

```
....
804.        syms_cache->data[syms_cache->nr].syms =
syms__load_pid(tgid);
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=19
Status	New

The size of the buffer used by syms__add_dso in PostfixExpr, at line 323 of iovisor@@bcc-0.29.0-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 *syms__load_file passes to buf, at line 656 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	680	342
Object	buf	PostfixExpr

Code Snippet

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
680.                          (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.              dso = &syms->dsos[syms->dso_sz++];
```

Buffer Overflow IndexFromInput\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=20
Status	New

The size of the buffer used by *ksyms__load in i, at line 96 of iovisor@@bcc-v0.21.0-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 *ksyms__load passes to f, at line 96 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	113	125
Object	f	i

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
113.              ret = fscanf(f, "%lx %c %s%*[^\n]\n",
....
125.              ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=21
Status	New

The size of the buffer used by *ksyms__load in i, at line 96 of iovisor@@bcc-v0.21.0-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 *ksyms__load passes to sym_name, at line 96 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	114	125
Object	sym_name	i

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
114.                          &sym_addr, &sym_type, sym_name);
....
125.              ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=22
Status	New

The size of the buffer used by syms__add_dso in i, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	320
Object	buf	i

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
320.                if (!strcmp(syms->dsos[i].name, name)) {
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=23
Status	New

The size of the buffer used by *syms_cache__get_syms in nr, at line 756 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Line	663	771
Object	buf	nr

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms_cache__get_syms(struct syms_cache *syms_cache, int tgid)

```
....
771.         syms_cache->data[syms_cache->nr].syms =
syms__load_pid(tgid);
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=24
Status	New

The size of the buffer used by syms__add_dso in PostfixExpr, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	332
Object	buf	PostfixExpr

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
332.                dso = &syms->dsos[syms->dso_sz++];
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=25
Status	New

The size of the buffer used by *ksyms__load in i, at line 96 of iovisor@@bcc-v0.23.0-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 *ksyms__load passes to f, at line 96 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	113	125
Object	f	i

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
113.                ret = fscanf(f, "%lx %c %s%*[^\n]\n",
....
125.                ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=26
Status	New

The size of the buffer used by *ksyms__load in i, at line 96 of iovisor@@bcc-v0.23.0-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 *ksyms__load passes to sym_name, at line 96 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	114	125
Object	sym_name	i

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
114.                            &sym_addr, &sym_type, sym_name);
....
125.                ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 14:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=27
Status New

The size of the buffer used by syms__add_dso in i, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	663	320
Object	buf	i

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
320.                if (!strcmp(syms->dsos[i].name, name)) {
```

Buffer Overflow IndexFromInput\Path 15:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=28
Status New

The size of the buffer used by *syms_cache__get_syms in nr, at line 756 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	663	771
Object	buf	nr

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method struct syms *syms_cache__get_syms(struct syms_cache *syms_cache, int tgid)

```
....
771.        syms_cache->data[syms_cache->nr].syms =
syms__load_pid(tgid);
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=29
Status	New

The size of the buffer used by syms__add_dso in PostfixExpr, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	663	332
Object	buf	PostfixExpr

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                        &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
332.              dso = &syms->dsos[syms->dso_sz++];
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=30
Status	New

The size of the buffer used by *ksyms__load in i, at line 97 of iovisor@@bcc-v0.25.0-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 *ksyms__load passes to f, at line 97 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	114	126
Object	f	i

Code Snippet

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method struct ksyms *ksyms__load(void)

```
....
114.              ret = fscanf(f, "%lx %c %s%*[^\n]\n",
....
126.              ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=31
Status	New

The size of the buffer used by *ksyms__load in i, at line 97 of iovisor@@bcc-v0.25.0-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 *ksyms__load passes to sym_name, at line 97 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	115	126
Object	sym_name	i

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
115.                            &sym_addr, &sym_type, sym_name);
....
126.                ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=32
Status	New

The size of the buffer used by syms__add_dso in i, at line 314 of iovisor@@bcc-v0.25.0-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 *syms__load_file passes to buf, at line 643 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	664	321
Object	buf	i

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
664.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
321.              if (!strcmp(syms->dsos[i].name, name)) {
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=33
Status	New

The size of the buffer used by *syms_cache__get_syms in nr, at line 757 of iovisor@@bcc-v0.25.0-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 *syms__load_file passes to buf, at line 643 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	664	772
Object	buf	nr

Code Snippet

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
664.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method struct syms *syms_cache__get_syms(struct syms_cache *syms_cache, int tgid)

```
....
772.        syms_cache->data[syms_cache->nr].syms =
syms__load_pid(tgid);
```

Buffer Overflow IndexFromInput\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=34
Status	New

The size of the buffer used by syms__add_dso in PostfixExpr, at line 314 of iovisor@@bcc-v0.25.0-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 *syms__load_file passes to buf, at line 643 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	664	333
Object	buf	PostfixExpr

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
664.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.                dso = &syms->dsos[syms->dso_sz++];
```

Buffer Overflow IndexFromInput\Path 22:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=35
Status New

The size of the buffer used by *ksyms__load in i, at line 98 of iovisor@@bcc-v0.30.0-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 *ksyms__load passes to f, at line 98 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	115	127
Object	f	i

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
115.                ret = fscanf(f, "%lx %c %s%*[^\n]\n",
....
127.                ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=36
Status	New

The size of the buffer used by *ksyms__load in i, at line 98 of iovisor@@bcc-v0.30.0-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 *ksyms__load passes to sym_name, at line 98 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	116	127
Object	sym_name	i

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
116.                            &sym_addr, &sym_type, sym_name);
....
127.                ksyms->syms[i].name += (unsigned long)ksyms->strs;
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=37
Status	New

The size of the buffer used by syms__add_dso in i, at line 323 of iovisor@@bcc-v0.30.0-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 *syms__load_file passes to buf, at line 657 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	681	330
Object	buf	i

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
681.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
330.              if (!strcmp(syms->dsos[i].name, name)) {
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=38
Status	New

The size of the buffer used by *syms_cache__get_syms in nr, at line 790 of iovisor@@bcc-v0.30.0-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 *syms__load_file passes to buf, at line 657 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	681	805
Object	buf	nr

Code Snippet

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
681.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method struct syms *syms_cache__get_syms(struct syms_cache *syms_cache, int tgid)

```
....
805.        syms_cache->data[syms_cache->nr].syms =
syms__load_pid(tgid);
```

Buffer Overflow IndexFromInput\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=39
Status	New

The size of the buffer used by syms__add_dso in PostfixExpr, at line 323 of iovisor@@bcc-v0.30.0-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 *syms__load_file passes to buf, at line 657 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	681	342
Object	buf	PostfixExpr

Code Snippet

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
681.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.                dso = &syms->dsos[syms->dso_sz++];
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=40
Status	New

The size of the buffer used by ilstin in gnum, at line 457 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that datain passes to data, at line 81 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	83	667
Object	data	gnum

Code Snippet

File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int datain(void *data, int size)

```
....
83.      if (fread(data, 1, size, g_fin) != size)
```

File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int ilstin(int size)

```
....
667.                     fprintf(stderr, "%s", genres[gnum]);
```

Buffer Overflow IndexFromInput\Path 28:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=41
Status New

The size of the buffer used by stringin in size, at line 88 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that datain passes to data, at line 81 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	83	95
Object	data	size

Code Snippet
File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int datain(void *data, int size)

```
....
83.      if (fread(data, 1, size, g_fin) != size)
```

File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int stringin(char *txt, int sizemax)

```
....
95.          if (!txt[size])
```

Buffer Overflow IndexFromInput\Path 29:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=42
Status	New

The size of the buffer used by stringin in size, at line 88 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stringin passes to BinaryExpr, at line 88 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	93	95
Object	BinaryExpr	size

Code Snippet
File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int stringin(char *txt, int sizemax)

```
....
93.          if (fread(txt + size, 1, 1, g_fin) != 1)
....
95.          if (!txt[size])
```

Buffer Overflow IndexFromInput\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=43
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	661	342
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=44
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	661	342
Object	Address	range_sz

Code Snippet

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=45
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	662	342
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
662.                            &map.file_off, &map.dev_major,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 33:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=46
Status New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	662	342
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
662.                            &map.file_off, &map.dev_major,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=47
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	342
Object	Address	range_sz

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 35:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=48
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	342
Object	Address	range_sz

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=49
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	661	343
Object	Address	range_sz

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.        dso->ranges[dso->range_sz].end = map->end_addr;
```

Buffer Overflow IndexFromInput\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=50
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	661	343
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.        dso->ranges[dso->range_sz].end = map->end_addr;
```

Buffer Overflow IndexFromInput\Path 38:

Severity High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=51
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	662	343
Object	Address	range_sz

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
662.                            &map.file_off, &map.dev_major,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.        dso->ranges[dso->range_sz].end = map->end_addr;
```

Buffer Overflow IndexFromInput\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=52
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	662	343
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
662.                            &map.file_off, &map.dev_major,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.        dso->ranges[dso->range_sz].end = map->end_addr;
```

Buffer Overflow IndexFromInput\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=53
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	343
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.        dso->ranges[dso->range_sz].end = map->end_addr;
```

Buffer Overflow IndexFromInput\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=54
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	343
Object	Address	range_sz

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.        dso->ranges[dso->range_sz].end = map->end_addr;
```

Buffer Overflow IndexFromInput\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=55
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	661	344

Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.        dso->ranges[dso->range_sz].file_off = map->file_off;
```

Buffer Overflow IndexFromInput\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=56
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	661	344
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.        dso->ranges[dso->range_sz].file_off = map->file_off;
```

Buffer Overflow IndexFromInput\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=57
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	662	344
Object	Address	range_sz

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
662.                            &map.file_off, &map.dev_major,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.        dso->ranges[dso->range_sz].file_off = map->file_off;
```

Buffer Overflow IndexFromInput\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=58
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	662	344
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
662.                            &map.file_off, &map.dev_major,
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.        dso->ranges[dso->range_sz].file_off = map->file_off;
```

Buffer Overflow IndexFromInput\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=59
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	344
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.        dso->ranges[dso->range_sz].file_off = map->file_off;
```

Buffer Overflow IndexFromInput\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=60
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	344
Object	Address	range_sz

Code Snippet

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.        dso->ranges[dso->range_sz].file_off = map->file_off;
```

Buffer Overflow IndexFromInput\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=61
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	661	342
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 49:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=62
Status New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	661	342
Object	Address	range_sz

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.                            &map.start_addr, &map.end_addr, perm,
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow IndexFromInput\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=63
Status	New

The size of the buffer used by syms__add_dso in range_sz, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to Address, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	662	342
Object	Address	range_sz

Code Snippet

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
662.                            &map.file_off, &map.dev_major,
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
342.        dso->ranges[dso->range_sz].start = map->start_addr;
```

Buffer Overflow boundedcpy

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundedcpy 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 boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1
Status	New

The size parameter sizeof in line 323 in file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c is influenced by the user input buf in line 656 in file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	680	343
Object	buf	sizeof

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
680.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.                memset(dso, 0, sizeof(*dso));
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2
Status	New

The size parameter sz in line 527 in file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c is influenced by the user input f in line 527 in file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	545	565
Object	f	sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
545.              ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
....
565.        memcpy(image, (void *)start_addr, sz);
```

Buffer Overflow boundedcpy\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3
Status	New

The size parameter sizeof in line 313 in file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c is influenced by the user input buf in line 642 in file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	333
Object	buf	sizeof

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.              memset(dso, 0, sizeof(*dso));
```

Buffer Overflow boundedcpy\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=4
Status	New

The size parameter sz in line 527 in file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c is influenced by the user input f in line 527 in file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	545	565
Object	f	sz

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
545.                ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
....
565.         memcpy(image, (void *)start_addr, sz);
```

Buffer Overflow boundedcpy\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=5
Status	New

The size parameter sizeof in line 313 in file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c is influenced by the user input buf in line 642 in file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	663	333
Object	buf	sizeof

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                          &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.              memset(dso, 0, sizeof(*dso));
```

Buffer Overflow boundedcpy\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=6
Status	New

The size parameter sz in line 528 in file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c is influenced by the user input f in line 528 in file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	546	566
Object	f	sz

Code Snippet

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.              ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
....
566.        memcpy(image, (void *)start_addr, sz);
```

Buffer Overflow boundedcpy\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=7
Status	New

The size parameter sizeof in line 314 in file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c is influenced by the user input buf in line 643 in file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	664	334
Object	buf	sizeof

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
664.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
334.                memset(dso, 0, sizeof(*dso));
```

Buffer Overflow boundedcpy\Path 8:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=8
Status New

The size parameter sizeof in line 323 in file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c is influenced by the user input buf in line 657 in file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	681	343
Object	buf	sizeof

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
681.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method	static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.              memset(dso, 0, sizeof(*dso));
```

Format String Attack

Query Path:
CPP\Cx\CPP Buffer Overflow\Format String Attack Version:1

Categories

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

Description

Format String Attack\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=9
Status	New

Method is_kernel_module at line 1005 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c receives the "%s %*s\n" value from user input. This value is then used to construct a "format string" "%s %*s\n", which is provided as an argument to a string formatting function in is_kernel_module method of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 1005.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1016	1016
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet	
File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	bool is_kernel_module(const char *name)

```
....
1016.             if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Format String Attack\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=10
Status	New

Method is_kernel_module at line 980 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c receives the "%s %*s\n" value from user input. This value is then used to construct a "format string" "%s %*s\n", which is

provided as an argument to a string formatting function in is_kernel_module method of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 980.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	991	991
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
991.            if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Format String Attack\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=11
Status New

Method is_kernel_module at line 980 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c receives the "%s %*s\n" value from user input. This value is then used to construct a "format string" "%s %*s\n", which is provided as an argument to a string formatting function in is_kernel_module method of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 980.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	991	991
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
991.            if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Format String Attack\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=12
Status New

Method is_kernel_module at line 971 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c receives the "%s %*s\n" value from user input. This value is then used to construct a "format string" "%s %*s\n", which is provided as an argument to a string formatting function in is_kernel_module method of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 971.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	982	982
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
982.              if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Format String Attack\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=13
Status	New

Method is_kernel_module at line 1006 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c receives the "%s %*s\n" value from user input. This value is then used to construct a "format string" "%s %*s\n", which is provided as an argument to a string formatting function in is_kernel_module method of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 1006.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1017	1017
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1017.             if (sscanf(buf, "%s %*s\n", buf) != 1)
```

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=1020038&projectid=20031&pathid=582
Status	New

The dangerous function, memcpy, was found in use at line 48 in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	82	82
Object	memcpy	memcpy

Code Snippet

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
82.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=583
Status	New

The dangerous function, memcpy, was found in use at line 538 in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	577	577
Object	memcpy	memcpy

Code Snippet

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method static int create_tmp_vdso_image(struct dso *dso)

```
....
577.        memcpy(image, (void *)start_addr, sz);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=584
Status	New

The dangerous function, memcpy, was found in use at line 46 in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	80	80
Object	memcpy	memcpy

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
80.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=585
Status	New

The dangerous function, memcpy, was found in use at line 527 in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	565	565
Object	memcpy	memcpy

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
565.        memcpy(image, (void *)start_addr, sz);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=586
Status	New

The dangerous function, memcpy, was found in use at line 46 in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	80	80
Object	memcpy	memcpy

Code Snippet	
File Name	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method	static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
80.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=587
Status	New

The dangerous function, memcpy, was found in use at line 527 in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	565	565
Object	memcpy	memcpy

Code Snippet

File Name	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
565.        memcpy(image, (void *)start_addr, sz);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=588
Status	New

The dangerous function, memcpy, was found in use at line 47 in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	81	81
Object	memcpy	memcpy

Code Snippet

File Name	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method	static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
81.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=589
Status	New

The dangerous function, memcpy, was found in use at line 528 in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	566	566
Object	memcpy	memcpy

Code Snippet	
File Name	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
566.        memcpy(image, (void *)start_addr, sz);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=590
Status	New

The dangerous function, memcpy, was found in use at line 48 in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	82	82
Object	memcpy	memcpy

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
82.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=591
Status	New

The dangerous function, memcpy, was found in use at line 538 in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	577	577
Object	memcpy	memcpy

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
577.        memcpy(image, (void *)start_addr, sz);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=592
Status	New

The dangerous function, memcpy, was found in use at line 131 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	143	143
Object	memcpy	memcpy

Code Snippet	
File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method	const char * x509_name (struct x509_certificate *cert) {

```
....
143.              memcpy ( buf, common_name->data, len );
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=593
Status	New

The dangerous function, memcpy, was found in use at line 168 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	175	175
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_version (struct x509_certificate *cert,

```
....
175.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=594
Status	New

The dangerous function, memcpy, was found in use at line 208 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	214	214
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_serial (struct x509_certificate *cert,

```
....
214.        memcpy ( &serial->raw, raw, sizeof ( serial->raw ) );
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=595
Status	New

The dangerous function, memcpy, was found in use at line 233 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	239	239
Object	memcpy	memcpy

Code Snippet

File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method	static int x509_parse_issuer (struct x509_certificate *cert,

```
....
239.        memcpy ( &issuer->raw, raw, sizeof ( issuer->raw ) );
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=596
Status	New

The dangerous function, memcpy, was found in use at line 258 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	267	267
Object	memcpy	memcpy

Code Snippet

File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method	static int x509_parse_validity (struct x509_certificate *cert,

```
....
267.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=597
Status	New

The dangerous function, memcpy, was found in use at line 301 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	309	309
Object	memcpy	memcpy

Code Snippet

File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c

Method	static int x509_parse_common_name (struct x509_certificate *cert,

```
....
309.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=598
Status	New

The dangerous function, memcpy, was found in use at line 301 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	316	316
Object	memcpy	memcpy

Code Snippet	
File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method	static int x509_parse_common_name (struct x509_certificate *cert,

```
....
316.              memcpy ( &oid_cursor, &cursor, sizeof ( oid_cursor )
);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=599
Status	New

The dangerous function, memcpy, was found in use at line 301 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	319	319
Object	memcpy	memcpy

Code Snippet	
File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c

Method	static int x509_parse_common_name (struct x509_certificate *cert,

```
....
319.              memcpy ( &name_cursor, &oid_cursor, sizeof (
name_cursor ) );
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=600
Status	New

The dangerous function, memcpy, was found in use at line 301 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	331	331
Object	memcpy	memcpy

Code Snippet	
File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method	static int x509_parse_common_name (struct x509_certificate *cert,

```
....
331.              memcpy ( &cert->subject.common_name, &name_cursor,
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=601
Status	New

The dangerous function, memcpy, was found in use at line 349 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	355	355
Object	memcpy	memcpy

Code Snippet	
File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c

Method	static int x509_parse_subject (struct x509_certificate *cert,

```
....
355.        memcpy ( &subject->raw, raw, sizeof ( subject->raw ) );
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=602
Status	New

The dangerous function, memcpy, was found in use at line 376 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	385	385
Object	memcpy	memcpy

Code Snippet	
File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method	static int x509_parse_public_key (struct x509_certificate *cert,

```
....
385.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=603
Status	New

The dangerous function, memcpy, was found in use at line 376 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	387	387
Object	memcpy	memcpy

Code Snippet	
File Name	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method	static int x509_parse_public_key (struct x509_certificate *cert,

```
....
387.        memcpy ( &public_key->raw, &cursor, sizeof ( public_key->raw
) );
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=604
Status	New

The dangerous function, memcpy, was found in use at line 421 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	430	430
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_basic_constraints (struct x509_certificate *cert,

```
....
430.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=605
Status	New

The dangerous function, memcpy, was found in use at line 542 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	551	551
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_key_purpose (struct x509_certificate *cert,

```
....
551.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=606
Status	New

The dangerous function, memcpy, was found in use at line 581 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	587	587
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_extended_key_usage (struct x509_certificate *cert,

```
....
587.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=607
Status	New

The dangerous function, memcpy, was found in use at line 607 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	614	614
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_ocsp (struct x509_certificate *cert,

```
....
614.        memcpy ( uri, raw, sizeof ( *uri ) );
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=608
Status	New

The dangerous function, memcpy, was found in use at line 667 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	675	675
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_access_description (struct x509_certificate *cert,

```
....
675.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=609
Status	New

The dangerous function, memcpy, was found in use at line 667 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	679	679
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_access_description (struct x509_certificate *cert,

```
....
679.        memcpy ( &subcursor, &cursor, sizeof ( subcursor ) );
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=610
Status	New

The dangerous function, memcpy, was found in use at line 700 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	706	706
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_authority_info_access (struct x509_certificate *cert,

```
....
706.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=611
Status	New

The dangerous function, memcpy, was found in use at line 727 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	734	734
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_subject_alt_name (struct x509_certificate *cert,

```
....
734.        memcpy ( names, raw, sizeof ( *names ) );
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=612
Status	New

The dangerous function, memcpy, was found in use at line 824 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	833	833
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_extension (struct x509_certificate *cert,

```
....
833.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=613
Status	New

The dangerous function, memcpy, was found in use at line 824 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	837	837
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_extension (struct x509_certificate *cert,

```
....
837.        memcpy ( &subcursor, &cursor, sizeof ( subcursor ) );
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=614
Status	New

The dangerous function, memcpy, was found in use at line 892 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	898	898
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_extensions (struct x509_certificate *cert,

```
....
898.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=615
Status	New

The dangerous function, memcpy, was found in use at line 919 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	926	926
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_tbscertificate (struct x509_certificate *cert,

```
....
926.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=616
Status	New

The dangerous function, memcpy, was found in use at line 919 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	928	928
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_tbscertificate (struct x509_certificate *cert,

```
....
928.        memcpy ( &cert->tbs, &cursor, sizeof ( cert->tbs ) );
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=617
Status	New

The dangerous function, memcpy, was found in use at line 989 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	998	998
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method int x509_parse (struct x509_certificate *cert,

```
....
998.        memcpy ( &cursor, raw, sizeof ( cursor ) );
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=618
Status	New

The dangerous function, memcpy, was found in use at line 989 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	999	999
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method int x509_parse (struct x509_certificate *cert,

```
....
999.        memcpy ( &cert->raw, &cursor, sizeof ( cert->raw ) );
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=619
Status	New

The dangerous function, memcpy, was found in use at line 1055 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1082	1082
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method int x509_certificate (const void *data, size_t len,

```
....
1082.       memcpy ( raw, cursor.data, cursor.len );
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=620
Status	New

The dangerous function, memcpy, was found in use at line 1487 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1494	1494
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_check_alt_name (struct x509_certificate *cert,

```
....
1494.       memcpy ( &alt_name, raw, sizeof ( alt_name ) );
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=621
Status	New

The dangerous function, memcpy, was found in use at line 1519 in ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1532	1532
Object	memcpy	memcpy

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c

Method	int x509_check_name (struct x509_certificate *cert, const char *name) {

```
....
1532.       memcpy ( &alt_name, &cert->extensions.alt_name.names,
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=622
Status	New

The dangerous function, memcpy, was found in use at line 256 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet	
File Name	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method	parse_packet(u_char *info, const struct pcap_pkthdr *header, const u_char *packet)

```
....
300.      memcpy(data, packet, header->caplen);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=623
Status	New

The dangerous function, memcpy, was found in use at line 414 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	599	599
Object	memcpy	memcpy

Code Snippet	
File Name	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method	capture_packet_reasm_ip(capture_info_t *capinfo, const struct pcap_pkthdr *header, u_char *packet, uint32_t *size, uint32_t *caplen)

```
....
599.              memcpy(packet + link_hl + ip_hl + (ntohs(frame_ip->ip_off) & IP_OFFMASK) * 8,
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=624
Status	New

The dangerous function, memcpy, was found in use at line 616 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	670	670
Object	memcpy	memcpy

Code Snippet	
File Name	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method	capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
670.              memcpy(new_payload, pkt->payload, pkt->payload_len);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=625
Status	New

The dangerous function, memcpy, was found in use at line 616 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c

Line	671	671
Object	memcpy	memcpy

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
671.                memcpy(new_payload + pkt->payload_len, payload,
size_payload);
```

Dangerous Functions\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=626
Status New

The dangerous function, memcpy, was found in use at line 616 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	674	674
Object	memcpy	memcpy

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
674.                memcpy(new_payload, payload, size_payload);
```

Dangerous Functions\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=627
Status New

The dangerous function, memcpy, was found in use at line 616 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	675	675
Object	memcpy	memcpy

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
675.              memcpy(new_payload + size_payload, pkt->payload, pkt->payload_len);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=628
Status	New

The dangerous function, memcpy, was found in use at line 616 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	683	683
Object	memcpy	memcpy

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
683.      memcpy(full_payload, pkt->payload, pkt->payload_len);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=629
Status	New

The dangerous function, memcpy, was found in use at line 718 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	787	787
Object	memcpy	memcpy

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_ws_check_packet(packet_t *packet)

```
....
787.          memcpy(ws_mask_key, (payload + ws_off), 4);
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=630
Status New

The dangerous function, memcpy, was found in use at line 718 in irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	797	797
Object	memcpy	memcpy

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_ws_check_packet(packet_t *packet)

```
....
797.      memcpy(newpayload, payload + ws_off, size_payload);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=631
Status New

The dangerous function, memcpy, was found in use at line 256 in irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Line	300	300
Object	memcpy	memcpy

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Method parse_packet(u_char *info, const struct pcap_pkthdr *header, const u_char *packet)

```
....
300.      memcpy(data, packet, header->caplen);
```

Use of Zero Initialized Pointer

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

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description
Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1436
Status	New

The variable declared in ret at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 111 is not initialized when it is used by charset at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 137.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	112	415
Object	ret	charset

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method char *long_arg(char *argv[], int i, int *j, int *n, char *prefix) {

```
....
112.    char *ret = NULL;
```

File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c

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

```
....
415.            charset = arg;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1437
Status	New

The variable declared in ret at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 111 is not initialized when it is used by timefmt at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 137.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	112	437
Object	ret	timefmt

Code Snippet

File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c

Method char *long_arg(char *argv[], int i, int *j, int *n, char *prefix) {

```
....
112.    char *ret = NULL;
```

File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c

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

```
....
437.            timefmt = scopy(arg);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1438
Status	New

The variable declared in ret at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 111 is not initialized when it is used by Hintro at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 137.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	112	515
Object	ret	Hintro

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method char *long_arg(char *argv[], int i, int *j, int *n, char *prefix) {

```
....
112.    char *ret = NULL;
```

File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
515.            Hintro = scopy(arg);
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1439
Status New

The variable declared in path at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 826 is not initialized when it is used by path at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 826.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	829	851
Object	path	path

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
829.    static char *path = NULL;
....
851.      if (strlen(dir)+strlen(ent->d_name)+2 > pathsize) path =
xrealloc(path,pathsize=(strlen(dir)+strlen(ent->d_name)+PATH_MAX));
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1440
Status	New

The variable declared in inf at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 894 is not initialized when it is used by inf at jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c in line 894.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	899	934
Object	inf	inf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
899.    struct infofile *inf = NULL;
....
934.    sav = dir = read_dir(d, &n, inf != NULL);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1441
Status	New

The variable declared in ret at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 111 is not initialized when it is used by charset at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 137.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	112	415
Object	ret	charset

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method char *long_arg(char *argv[], int i, int *j, int *n, char *prefix) {

```
....
112.    char *ret = NULL;
```

File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c

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

```
....
415.            charset = arg;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1442
Status	New

The variable declared in ret at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 111 is not initialized when it is used by timefmt at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 137.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	112	437
Object	ret	timefmt

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method char *long_arg(char *argv[], int i, int *j, int *n, char *prefix) {

```
....
112.    char *ret = NULL;
```

File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c

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

```
....
437.            timefmt = scopy(arg);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1443
Status	New

The variable declared in ret at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 111 is not initialized when it is used by Hintro at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 137.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	112	515
Object	ret	Hintro

Code Snippet

File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c

Method char *long_arg(char *argv[], int i, int *j, int *n, char *prefix) {

```
....
112.    char *ret = NULL;
```

File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c

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

```
....
515.              Hintro = scopy(arg);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1444
Status	New

The variable declared in path at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 826 is not initialized when it is used by path at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 826.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	829	851
Object	path	path

Code Snippet

File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c

Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
829.    static char *path = NULL;
....
851.      if (strlen(dir)+strlen(ent->d_name)+2 > pathsize) path =
xrealloc(path,pathsize=(strlen(dir)+strlen(ent->d_name)+PATH_MAX));
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1445
Status	New

The variable declared in inf at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 894 is not initialized when it is used by inf at jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c in line 894.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	899	934
Object	inf	inf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
899.    struct infofile *inf = NULL;
....
934.    sav = dir = read_dir(d, &n, inf != NULL);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1446
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1276 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1344	1431

Object	extendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::BuildXrefTableAndTrailerFromXrefStream(long long inXrefStreamObjectID)

```
....
1344.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                  XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1447
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 458 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	480	1431
Object	extendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::BuildXrefTableFromTable()

```
....
480.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                    XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1448
Status	New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1442	1431
Object	outExtendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.       outExtendedTable = NULL;
....
1431.                                                    XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1449
Status	New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	558	1431
Object	Pointer	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.        *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                   XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1450
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1033 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1049	1431
Object	extendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousXrefs(PDFDictionary* inTrailer)

```
....
1049.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                   XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1451
Status	New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by mXrefTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1202.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	558	1215
Object	Pointer	mXrefTable

Code Snippet

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.      *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method void PDFParser::MergeXrefWithMainXref(XrefEntryInput* inTableToMerge,ObjectIDType inMergedTableSize)

```
....
1215.                   mXrefTable[i] =   inTableToMerge[i];
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1452
Status	New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by mXrefTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1202.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1442	1215

Object	outExtendedTable	mXrefTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.       outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method void PDFParser::MergeXrefWithMainXref(XrefEntryInput* inTableToMerge,ObjectIDType inMergedTableSize)

```
....
1215.                   mXrefTable[i] =   inTableToMerge[i];
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1453
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1033 is not initialized when it is used by mXrefTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1202.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1049	1215
Object	extendedTable	mXrefTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousXrefs(PDFDictionary* inTrailer)

```
....
1049.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method void PDFParser::MergeXrefWithMainXref(XrefEntryInput* inTableToMerge,ObjectIDType inMergedTableSize)

```
....
1215.                    mXrefTable[i] =   inTableToMerge[i];
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1454
Status	New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1442	1505
Object	outExtendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.      outExtendedTable = NULL;
....
1505.                      *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1455
Status	New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	558	1505
Object	Pointer	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.      *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1505.                     *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1456
Status	New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1442	1551
Object	outExtendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.      outExtendedTable = NULL;
....
1551.                          *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1457
Status	New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	558	1551
Object	Pointer	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.      *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1551.                          *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1458
Status New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1033 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1049	1551
Object	extendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousXrefs(PDFDictionary* inTrailer)

```
....
1049.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1551.                           *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1459
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1920.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1109	2017
Object	trailerDictionary	result

Code Snippet

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2017.                   result =
mDecryptionHelper.CreateDecryptionFilterForStream(inPDFStream, inStream,
cryptFilterName->GetValue());
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=1460
Status	New

The variable declared in result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1920 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	2040	1885
Object	result	result

Code Snippet

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2040.              result = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1885.                                  result = createStatus.second;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1461
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1920.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1109	2021
Object	trailerDictionary	result

Code Snippet

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method	EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method	EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2021.                   result = mParserExtender-
>CreateFilterForStream(inStream,inFilterName,inDecodeParams,
inPDFStream);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1462
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by widthsArray at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1109	1476
Object	trailerDictionary	widthsArray

Code Snippet

File Name	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method	EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method	EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1476.                   widthsArray[i] = (int)widthObject->GetValue();
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1463
Status	New

The variable declared in result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1920 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	2040	1899
Object	result	result

Code Snippet

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2040.              result = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1899.                          result = createStatus.second;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1464
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Line	1109	1844
Object	trailerDictionary	result

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1844.               result = WrapWithDecryptionFilter(inStream,result);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1465
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1109	1842
Object	trailerDictionary	result

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Method IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1842.             result = new InputLimitedStream(mStream,lengthObject-
>GetValue(),false);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1466
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 458 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	480	1431
Object	extendedTable	outExtendedTable

Code Snippet

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::BuildXrefTableFromTable()

```
....
480.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                 XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1467
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1276 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1344	1431
Object	extendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::BuildXrefTableAndTrailerFromXrefStream(long long inXrefStreamObjectID)

```
....
1344.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                  XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1468
Status New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1442	1431
Object	outExtendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.      outExtendedTable = NULL;
....
1431.                                                    XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1469
Status	New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	558	1431
Object	Pointer	outExtendedTable

Code Snippet

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.      *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                    XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1470
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1033 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1049	1431
Object	extendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousXrefs(PDFDictionary* inTrailer)

```
....
1049.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1431.                                                  XrefEntryInput**
outExtendedTable,
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1471
Status	New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by mXrefTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1202.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	558	1215
Object	Pointer	mXrefTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.       *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method	void PDFParser::MergeXrefWithMainXref(XrefEntryInput* inTableToMerge,ObjectIDType inMergedTableSize)

```
....
1215.                   mXrefTable[i] =   inTableToMerge[i];
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1472
Status	New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by mXrefTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1202.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1442	1215
Object	outExtendedTable	mXrefTable

Code Snippet	
File Name	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method	EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.       outExtendedTable = NULL;
```

File Name	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method	void PDFParser::MergeXrefWithMainXref(XrefEntryInput* inTableToMerge,ObjectIDType inMergedTableSize)

```
....
1215.                   mXrefTable[i] =   inTableToMerge[i];
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1473
Status	New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1033 is not initialized when it is used by mXrefTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1202.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1049	1215
Object	extendedTable	mXrefTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousXrefs(PDFDictionary* inTrailer)

```
....
1049.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method void PDFParser::MergeXrefWithMainXref(XrefEntryInput* inTableToMerge,ObjectIDType inMergedTableSize)

```
....
1215.                   mXrefTable[i] =   inTableToMerge[i];
```

Use of Zero Initialized Pointer\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1474
Status New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1442	1505
Object	outExtendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.      outExtendedTable = NULL;
....
1505.                      *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1475
Status	New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	558	1505
Object	Pointer	outExtendedTable

Code Snippet

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.      *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1505.                     *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1476
Status	New

The variable declared in outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1442	1551
Object	outExtendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1442.      outExtendedTable = NULL;
....
1551.                          *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1477
Status New

The variable declared in Pointer at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 542 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	558	1551
Object	Pointer	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefTable(XrefEntryInput* inXrefTable,

```
....
558.      *outExtendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1551.                          *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1478
Status New

The variable declared in extendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1033 is not initialized when it is used by outExtendedTable at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1049	1551
Object	extendedTable	outExtendedTable

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousXrefs(PDFDictionary* inTrailer)

```
....
1049.          XrefEntryInput* extendedTable = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1551.                          *outExtendedTable = inXrefTable;
```

Use of Zero Initialized Pointer\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1479
Status New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1920.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1109	2017
Object	trailerDictionary	result

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2017.                   result =
mDecryptionHelper.CreateDecryptionFilterForStream(inPDFStream, inStream,
cryptFilterName->GetValue());
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1480
Status	New

The variable declared in result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1920 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	2040	1885
Object	result	result

Code Snippet

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2040.               result = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1885.                                   result = createStatus.second;
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1481
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1920.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1109	2021
Object	trailerDictionary	result

Code Snippet

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                    PDFDictionary* trailerDictionary = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c

Method EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2021.                    result = mParserExtender-
>CreateFilterForStream(inStream,inFilterName,inDecodeParams,
inPDFStream);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1482
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by widthsArray at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1428.

	Source	Destination

File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1109	1476
Object	trailerDictionary	widthsArray

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParseXrefFromXrefStream(XrefEntryInput* inXrefTable,

```
....
1476.                   widthsArray[i] = (int)widthObject->GetValue();
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1483
Status	New

The variable declared in result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1920 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	2040	1899
Object	result	result

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCodeAndIByteReader PDFParser::CreateFilterForStream(IByteReader* inStream,PDFName* inFilterName,PDFDictionary* inDecodeParams, PDFStreamInput* inPDFStream)

```
....
2040.               result = NULL;
```

File Name	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method	IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1899.                           result = createStatus.second;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1484
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1109	1844
Object	trailerDictionary	result

Code Snippet

File Name	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method	EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
```

File Name	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method	IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1844.             result = WrapWithDecryptionFilter(inStream,result);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1485
Status	New

The variable declared in trailerDictionary at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by result at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1824.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1109	1842
Object	trailerDictionary	result

Code Snippet
File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                    PDFDictionary* trailerDictionary = NULL;
```

File Name julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method IByteReader* PDFParser::CreateInputStreamReader(PDFStreamInput* inStream)

```
....
1842.              result = new InputLimitedStream(mStream,lengthObject-
>GetValue(),false);
```

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=1020038&projectid=20031&pathid=107
Status	New

The size of the buffer used by x509_parse_serial in ->, at line 208 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that x509_parse_serial passes to ->, at line 208 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c

Line	214	214
Object	->	->

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_serial (struct x509_certificate *cert,

```
....
214.        memcpy ( &serial->raw, raw, sizeof ( serial->raw ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=108
Status	New

The size of the buffer used by x509_parse_issuer in ->, at line 233 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that x509_parse_issuer passes to ->, at line 233 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	239	239
Object	->	->

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_issuer (struct x509_certificate *cert,

```
....
239.        memcpy ( &issuer->raw, raw, sizeof ( issuer->raw ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=109
Status	New

The size of the buffer used by x509_parse_common_name in Namespace1227777157, at line 301 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that x509_parse_common_name passes to Namespace1227777157, at line 301 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination

File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	332	332
Object	Namespace1227777157	Namespace1227777157

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_common_name (struct x509_certificate *cert,

```
....
332.                    sizeof ( cert->subject.common_name ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=110
Status	New

The size of the buffer used by x509_parse_subject in ->, at line 349 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that x509_parse_subject passes to ->, at line 349 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	355	355
Object	->	->

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_subject (struct x509_certificate *cert,

```
....
355.        memcpy ( &subject->raw, raw, sizeof ( subject->raw ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=111
Status	New

The size of the buffer used by x509_parse_public_key in ->, at line 376 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that x509_parse_public_key passes to ->, at line 376 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	387	387
Object	->	->

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_public_key (struct x509_certificate *cert,

```
....
387.         memcpy ( &public_key->raw, &cursor, sizeof ( public_key->raw
) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=112
Status New

The size of the buffer used by x509_parse_tbscertificate in ->, at line 919 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that x509_parse_tbscertificate passes to ->, at line 919 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	928	928
Object	->	->

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static int x509_parse_tbscertificate (struct x509_certificate *cert,

```
....
928.         memcpy ( &cert->tbs, &cursor, sizeof ( cert->tbs ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=113
Status New

The size of the buffer used by x509_parse in ->, at line 989 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that x509_parse passes to ->, at line 989 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	999	999
Object	->	->

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method int x509_parse (struct x509_certificate *cert,

```
....
999.        memcpy ( &cert->raw, &cursor, sizeof ( cert->raw ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=114
Status New

The size of the buffer used by window_manager_make_key_window in uint32_t, at line 817 of koekeishiya@@yabai-v4.0.0-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 window_manager_make_key_window passes to uint32_t, at line 817 of koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	822	822
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Method static void window_manager_make_key_window(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
822.      memcpy(bytes1 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=115
Status New

The size of the buffer used by window_manager_make_key_window in uint32_t, at line 817 of koekeishiya@@yabai-v4.0.0-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 window_manager_make_key_window passes to uint32_t, at line 817 of koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	825	825
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Method static void window_manager_make_key_window(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
825.      memcpy(bytes2 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=116
Status	New

The size of the buffer used by window_manager_focus_window_without_raise in uint32_t, at line 832 of koekeishiya@@yabai-v4.0.0-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 window_manager_focus_window_without_raise passes to uint32_t, at line 832 of koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	836	836
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Method void window_manager_focus_window_without_raise(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
836.          memcpy(bytes1 + 0x3c, &g_window_manager.focused_window_id,
sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=117
Status	New

The size of the buffer used by window_manager_focus_window_without_raise in uint32_t, at line 832 of koekeishiya@@yabai-v4.0.0-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 window_manager_focus_window_without_raise passes to uint32_t, at line 832 of koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	846	846
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Method void window_manager_focus_window_without_raise(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
846.          memcpy(bytes2 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=118
Status	New

The size of the buffer used by window_manager_make_key_window in uint32_t, at line 816 of koekeishiya@@yabai-v4.0.2-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 window_manager_make_key_window passes to uint32_t, at line 816 of koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	821	821
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Method static void window_manager_make_key_window(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
821.      memcpy(bytes1 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=119
Status	New

The size of the buffer used by window_manager_make_key_window in uint32_t, at line 816 of koekeishiya@@yabai-v4.0.2-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 window_manager_make_key_window passes to uint32_t, at line 816 of koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	824	824
Object	uint32_t	uint32_t

Code Snippet

File Name koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c

Method static void window_manager_make_key_window(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
824.      memcpy(bytes2 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=120
Status	New

The size of the buffer used by window_manager_focus_window_without_raise in uint32_t, at line 831 of koekeishiya@@yabai-v4.0.2-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 window_manager_focus_window_without_raise passes to uint32_t, at line 831 of koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	835	835
Object	uint32_t	uint32_t

Code Snippet	
File Name	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Method	void window_manager_focus_window_without_raise(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
835.          memcpy(bytes1 + 0x3c, &g_window_manager.focused_window_id,
sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=121
Status	New

The size of the buffer used by window_manager_focus_window_without_raise in uint32_t, at line 831 of koekeishiya@@yabai-v4.0.2-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 window_manager_focus_window_without_raise passes to uint32_t, at line 831 of koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	845	845
Object	uint32_t	uint32_t

Code Snippet	
File Name	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Method	void window_manager_focus_window_without_raise(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
845.          memcpy(bytes2 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=122
Status	New

The size of the buffer used by window_manager_make_key_window in uint32_t, at line 1198 of koekeishiya@@yabai-v5.0.7-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 window_manager_make_key_window passes to uint32_t, at line 1198 of koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination

File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1219	1219
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method static void window_manager_make_key_window(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
1219.       memcpy(bytes1 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=123
Status	New

The size of the buffer used by window_manager_make_key_window in uint32_t, at line 1198 of koekeishiya@@yabai-v5.0.7-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 window_manager_make_key_window passes to uint32_t, at line 1198 of koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1222	1222
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method static void window_manager_make_key_window(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
1222.       memcpy(bytes2 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=124
Status	New

The size of the buffer used by window_manager_focus_window_without_raise in uint32_t, at line 1229 of koekeishiya@@yabai-v5.0.7-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 window_manager_focus_window_without_raise passes to uint32_t, at line 1229 of koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1245	1245
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method void window_manager_focus_window_without_raise(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
1245.          memcpy(bytes1 + 0x3c,
&g_window_manager.focused_window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=125
Status New

The size of the buffer used by window_manager_focus_window_without_raise in uint32_t, at line 1229 of koekeishiya@@yabai-v5.0.7-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 window_manager_focus_window_without_raise passes to uint32_t, at line 1229 of koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1258	1258
Object	uint32_t	uint32_t

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method void window_manager_focus_window_without_raise(ProcessSerialNumber *window_psn, uint32_t window_id)

```
....
1258.          memcpy(bytes2 + 0x3c, &window_id, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=126
Status	New

The size of the buffer used by *getinfo in _info, at line 734 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *getinfo passes to _info, at line 734 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	773	773
Object	_info	_info

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info *getinfo(char *name, char *path)

```
....
773.    memset(ent, 0, sizeof(struct _info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=127
Status	New

The size of the buffer used by *getinfo in _info, at line 734 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *getinfo passes to _info, at line 734 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	773	773
Object	_info	_info

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info *getinfo(char *name, char *path)

```
....
773.    memset(ent, 0, sizeof(struct _info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=128
Status	New

The size of the buffer used by process_tgs_req in Namespace497186214, at line 101 of krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process_tgs_req passes to Namespace497186214, at line 101 of krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c
Line	606	606
Object	Namespace497186214	Namespace497186214

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c
Method process_tgs_req(krb5_kdc_req *request, krb5_data *pkt,

```
....
606.          memset(&enc_tkt_reply.transited, 0,
sizeof(enc_tkt_reply.transited));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=129
Status	New

The size of the buffer used by xdr_krb5_key_data_nocontents in krb5_key_data, at line 244 of krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xdr_krb5_key_data_nocontents passes to krb5_key_data, at line 244 of krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Line	254	254
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Method bool_t xdr_krb5_key_data_nocontents(XDR *xdrs, krb5_key_data *objp)

```
....
254.          memset(objp, 0, sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=130
Status	New

The size of the buffer used by krb5_db_delete_principal in kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_db_delete_principal passes to kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1010	1010
Object	kdb_incr_update_t	kdb_incr_update_t

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1010.      memset(&upd, 0, sizeof(kdb_incr_update_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=131
Status	New

The size of the buffer used by krb5_dbe_create_key_data in krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_dbe_create_key_data passes to krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1542	1542
Object	krb5_key_data	krb5_key_data

Code Snippet	
File Name	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method	krb5_dbe_create_key_data(krb5_context context, krb5_db_entry *entry)

```
....
1542.       memset(entry->key_data + entry->n_key_data, 0,
sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=132
Status	New

The size of the buffer used by process_tgs_req in Namespace994109596, at line 101 of krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process_tgs_req passes to Namespace994109596, at line 101 of krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c
Line	606	606
Object	Namespace994109596	Namespace994109596

Code Snippet	
File Name	krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c
Method	process_tgs_req(krb5_kdc_req *request, krb5_data *pkt,

```
....
606.           memset(&enc_tkt_reply.transited, 0,
sizeof(enc_tkt_reply.transited));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=133
Status	New

The size of the buffer used by xdr_krb5_key_data_nocontents in krb5_key_data, at line 244 of krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xdr_krb5_key_data_nocontents passes to krb5_key_data, at line 244 of krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c

Line	254	254
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Method bool_t xdr_krb5_key_data_nocontents(XDR *xdrs, krb5_key_data *objp)

```
....
254.          memset(objp, 0, sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=134
Status	New

The size of the buffer used by krb5_db_delete_principal in kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_db_delete_principal passes to kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1010	1010
Object	kdb_incr_update_t	kdb_incr_update_t

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1010.      memset(&upd, 0, sizeof(kdb_incr_update_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=135
Status	New

The size of the buffer used by krb5_dbe_create_key_data in krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_dbe_create_key_data passes to krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1542	1542
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_create_key_data(krb5_context context, krb5_db_entry *entry)

```
....
1542.      memset(entry->key_data + entry->n_key_data, 0,
sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=136
Status	New

The size of the buffer used by xdr_krb5_key_data_nocontents in krb5_key_data, at line 244 of krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xdr_krb5_key_data_nocontents passes to krb5_key_data, at line 244 of krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Line	254	254
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Method bool_t xdr_krb5_key_data_nocontents(XDR *xdrs, krb5_key_data *objp)

```
....
254.          memset(objp, 0, sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=137
Status	New

The size of the buffer used by krb5_db_delete_principal in kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_db_delete_principal passes to kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1010	1010
Object	kdb_incr_update_t	kdb_incr_update_t

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1010.       memset(&upd, 0, sizeof(kdb_incr_update_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=138
Status New

The size of the buffer used by krb5_dbe_create_key_data in krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_dbe_create_key_data passes to krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1542	1542
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_dbe_create_key_data(krb5_context context, krb5_db_entry *entry)

```
....
1542.       memset(entry->key_data + entry->n_key_data, 0,
sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=139
Status	New

The size of the buffer used by process_tgs_req in Namespace1439156903, at line 101 of krb5@@krb5-krb5-1.19.1-final-CVE-2021-37750-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process_tgs_req passes to Namespace1439156903, at line 101 of krb5@@krb5-krb5-1.19.1-final-CVE-2021-37750-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2021-37750-TP.c
Line	577	577
Object	Namespace1439156903	Namespace1439156903

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2021-37750-TP.c
Method process_tgs_req(krb5_kdc_req *request, krb5_data *pkt,

```
....
577.          memset(&enc_tkt_reply.transited, 0,
sizeof(enc_tkt_reply.transited));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=140
Status	New

The size of the buffer used by xdr_krb5_key_data_nocontents in krb5_key_data, at line 244 of krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xdr_krb5_key_data_nocontents passes to krb5_key_data, at line 244 of krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c
Line	254	254
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c
Method bool_t xdr_krb5_key_data_nocontents(XDR *xdrs, krb5_key_data *objp)

```
....
254.          memset(objp, 0, sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=141
Status	New

The size of the buffer used by krb5_db_delete_principal in kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_db_delete_principal passes to kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1010	1010
Object	kdb_incr_update_t	kdb_incr_update_t

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1010.       memset(&upd, 0, sizeof(kdb_incr_update_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=142
Status	New

The size of the buffer used by krb5_dbe_create_key_data in krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_dbe_create_key_data passes to krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1542	1542
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_dbe_create_key_data(krb5_context context, krb5_db_entry *entry)

```
....
1542.       memset(entry->key_data + entry->n_key_data, 0,
sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=143
Status	New

The size of the buffer used by process_tgs_req in Namespace1091310852, at line 101 of krb5@@krb5-krb5-1.19.2-final-CVE-2021-37750-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that process_tgs_req passes to Namespace1091310852, at line 101 of krb5@@krb5-krb5-1.19.2-final-CVE-2021-37750-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2021-37750-TP.c
Line	577	577
Object	Namespace1091310852	Namespace1091310852

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2021-37750-TP.c
Method process_tgs_req(krb5_kdc_req *request, krb5_data *pkt,

```
....
577.           memset(&enc_tkt_reply.transited, 0,
sizeof(enc_tkt_reply.transited));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=144
Status	New

The size of the buffer used by xdr_krb5_key_data_nocontents in krb5_key_data, at line 244 of krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xdr_krb5_key_data_nocontents passes to krb5_key_data, at line 244 of krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c
Line	254	254
Object	krb5_key_data	krb5_key_data

Code Snippet	
File Name	krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c
Method	bool_t xdr_krb5_key_data_nocontents(XDR *xdrs, krb5_key_data *objp)

```
....
254.          memset(objp, 0, sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=145
Status	New

The size of the buffer used by krb5_db_delete_principal in kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_db_delete_principal passes to kdb_incr_update_t, at line 996 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Line	1010	1010
Object	kdb_incr_update_t	kdb_incr_update_t

Code Snippet	
File Name	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Method	krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1010.      memset(&upd, 0, sizeof(kdb_incr_update_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=146
Status	New

The size of the buffer used by krb5_dbe_create_key_data in krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that krb5_dbe_create_key_data passes to krb5_key_data, at line 1532 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c

Line	1542	1542
Object	krb5_key_data	krb5_key_data

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Method krb5_dbe_create_key_data(krb5_context context, krb5_db_entry *entry)

```
....
1542.      memset(entry->key_data + entry->n_key_data, 0,
sizeof(krb5_key_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=147
Status	New

The size of the buffer used by ksyms__add_symbol in name_len, at line 48 of iovisor@@bcc-0.29.0-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 ksyms__add_symbol passes to name_len, at line 48 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	82	82
Object	name_len	name_len

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
82.   memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=148
Status	New

The size of the buffer used by ksyms__add_symbol in name_len, at line 46 of iovisor@@bcc-v0.21.0-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 ksyms__add_symbol passes to name_len, at line 46 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	80	80
Object	name_len	name_len

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
80.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=149
Status New

The size of the buffer used by ksyms__add_symbol in name_len, at line 46 of iovisor@@bcc-v0.23.0-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 ksyms__add_symbol passes to name_len, at line 46 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	80	80
Object	name_len	name_len

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
80.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=150
Status New

The size of the buffer used by ksyms__add_symbol in name_len, at line 47 of iovisor@@bcc-v0.25.0-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 ksyms__add_symbol passes to name_len, at line 47 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	81	81
Object	name_len	name_len

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
81.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=151
Status New

The size of the buffer used by ksyms__add_symbol in name_len, at line 48 of iovisor@@bcc-v0.30.0-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 ksyms__add_symbol passes to name_len, at line 48 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	82	82
Object	name_len	name_len

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
82.    memcpy(ksyms->strs + ksyms->strs_sz, name, name_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=152
Status	New

The size of the buffer used by x509_certificate in cursor, at line 1055 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that x509_certificate passes to cursor, at line 1055 of ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c, to overwrite the target buffer.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1082	1082
Object	cursor	cursor

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method int x509_certificate (const void *data, size_t len,

```
....
1082.       memcpy ( raw, cursor.data, cursor.len );
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=153
Status	New

The size of the buffer used by parse_packet in header, at line 256 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_packet passes to header, at line 256 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, to overwrite the target buffer.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	300	300
Object	header	header

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method parse_packet(u_char *info, const struct pcap_pkthdr *header, const u_char *packet)

```
....
300.      memcpy(data, packet, header->caplen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=154
Status	New

The size of the buffer used by capture_packet_reasm_tcp in pkt, at line 616 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that capture_packet_reasm_tcp passes to pkt, at line 616 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, to overwrite the target buffer.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	670	670
Object	pkt	pkt

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
670.              memcpy(new_payload, pkt->payload, pkt->payload_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=155
Status	New

The size of the buffer used by capture_packet_reasm_tcp in size_payload, at line 616 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that capture_packet_reasm_tcp passes to size_payload, at line 616 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, to overwrite the target buffer.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	671	671
Object	size_payload	size_payload

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
671.              memcpy(new_payload + pkt->payload_len, payload,
size_payload);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=156
Status	New

The size of the buffer used by capture_packet_reasm_tcp in size_payload, at line 616 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that capture_packet_reasm_tcp passes to size_payload, at line 616 of irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c, to overwrite the target buffer.

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	674	674
Object	size_payload	size_payload

Code Snippet

File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c

Method capture_packet_reasm_tcp(capture_info_t *capinfo, packet_t *packet, struct tcphdr *tcp, u_char *payload, int size_payload) {

```
....
674.              memcpy(new_payload, payload, size_payload);
```

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=1020038&projectid=20031&pathid=1315
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Line	974	974
Object	j	j

Code Snippet

File Name	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Method	mspac_get_attribute_types(krb5_context kcontext,

```
....
974.                length = asprintf(&attrs[j].data, "urn:mspac:%d",
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1316
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Line	974	974
Object	j	j

Code Snippet

File Name	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Method	mspac_get_attribute_types(krb5_context kcontext,

```
....
974.                length = asprintf(&attrs[j].data, "urn:mspac:%d",
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1317
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Line	974	974
Object	j	j

Code Snippet

File Name	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Method	mspac_get_attribute_types(krb5_context kcontext,

```
....
974.                length = asprintf(&attrs[j].data, "urn:mspac:%d",
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1318
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Line	974	974
Object	j	j

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Method mspac_get_attribute_types(krb5_context kcontext,

```
....
974.                length = asprintf(&attrs[j].data, "urn:mspac:%d",
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1319
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Line	974	974
Object	j	j

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Method mspac_get_attribute_types(krb5_context kcontext,

```
....
974.                length = asprintf(&attrs[j].data, "urn:mspac:%d",
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1320
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	598	598
Object	context	context

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method void window_manager_animate_window_list_async(struct window_capture *window_list, int window_count)

```
....
598.      struct window_animation_context *context =
malloc(sizeof(struct window_animation_context));
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1321
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	110	110
Object	ksyms	ksyms

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
110.        ksyms = calloc(1, sizeof(*ksyms));
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1322
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Line	344	344
Object	name	name

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.              dso->name = strdup(name);
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1323
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	669	669
Object	syms	syms

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
669.        syms = calloc(1, sizeof(*syms));
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1324
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	768	768
Object	syms_cache	syms_cache

Code Snippet

File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	struct syms_cache *syms_cache__new(int nr)

```
....
768.        syms_cache = calloc(1, sizeof(*syms_cache));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1325
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	772	772
Object	data	data

Code Snippet

File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	struct syms_cache *syms_cache__new(int nr)

```
....
772.             syms_cache->data = calloc(nr, sizeof(*syms_cache-
>data));
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1326
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	826	826
Object	name	name

Code Snippet

File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	static int partitions__add_partition(struct partitions *partitions,

```
....
826.        partition->name = strdup(name);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1327
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	846	846
Object	partitions	partitions

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
846.        partitions = calloc(1, sizeof(*partitions));
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1328
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	108	108
Object	ksyms	ksyms

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
108.        ksyms = calloc(1, sizeof(*ksyms));
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1329

Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	334	334
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
334.                dso->name = strdup(name);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1330
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	655	655
Object	syms	syms

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
655.        syms = calloc(1, sizeof(*syms));
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1331
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Line	735	735
Object	syms_cache	syms_cache

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms_cache *syms_cache__new(int nr)

```
....
735.        syms_cache = calloc(1, sizeof(*syms_cache));
```

Memory Leak\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1332
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	739	739
Object	data	data

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms_cache *syms_cache__new(int nr)

```
....
739.                syms_cache->data = calloc(nr, sizeof(*syms_cache-
>data));
```

Memory Leak\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1333
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	793	793
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method	static int partitions__add_partition(struct partitions *partitions,

```
....
793.        partition->name = strdup(name);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1334
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	813	813
Object	partitions	partitions

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
813.        partitions = calloc(1, sizeof(*partitions));
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1335
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	108	108
Object	ksyms	ksyms

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
108.        ksyms = calloc(1, sizeof(*ksyms));
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1336
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	334	334
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
334.              dso->name = strdup(name);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1337
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	655	655
Object	syms	syms

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
655.        syms = calloc(1, sizeof(*syms));
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1338
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	735	735
Object	syms_cache	syms_cache

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms_cache *syms_cache__new(int nr)

```
....
735.        syms_cache = calloc(1, sizeof(*syms_cache));
```

Memory Leak\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1339
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	739	739
Object	data	data

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms_cache *syms_cache__new(int nr)

```
....
739.              syms_cache->data = calloc(nr, sizeof(*syms_cache-
>data));
```

Memory Leak\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1340
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Line	793	793
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int partitions__add_partition(struct partitions *partitions,

```
....
793.        partition->name = strdup(name);
```

Memory Leak\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1341
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	813	813
Object	partitions	partitions

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
813.        partitions = calloc(1, sizeof(*partitions));
```

Memory Leak\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1342
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	109	109
Object	ksyms	ksyms

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method	struct ksyms *ksyms__load(void)

```
....
109.        ksyms = calloc(1, sizeof(*ksyms));
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1343
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	335	335
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
335.              dso->name = strdup(name);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1344
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	656	656
Object	syms	syms

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
656.        syms = calloc(1, sizeof(*syms));
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1345
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	736	736
Object	syms_cache	syms_cache

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms_cache *syms_cache__new(int nr)

```
....
736.        syms_cache = calloc(1, sizeof(*syms_cache));
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1346
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	740	740
Object	data	data

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms_cache *syms_cache__new(int nr)

```
....
740.                syms_cache->data = calloc(nr, sizeof(*syms_cache-
>data));
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1347

Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	794	794
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int partitions__add_partition(struct partitions *partitions,

```
....
794.        partition->name = strdup(name);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1348
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	814	814
Object	partitions	partitions

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
814.        partitions = calloc(1, sizeof(*partitions));
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1349
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Line	110	110
Object	ksyms	ksyms

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
110.        ksyms = calloc(1, sizeof(*ksyms));
```

Memory Leak\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1350
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	344	344
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
344.              dso->name = strdup(name);
```

Memory Leak\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1351
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	670	670
Object	syms	syms

Code Snippet

File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	struct syms *syms__load_file(const char *fname)

```
....
670.        syms = calloc(1, sizeof(*syms));
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1352
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	769	769
Object	syms_cache	syms_cache

Code Snippet

File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	struct syms_cache *syms_cache__new(int nr)

```
....
769.        syms_cache = calloc(1, sizeof(*syms_cache));
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1353
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	773	773
Object	data	data

Code Snippet

File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	struct syms_cache *syms_cache__new(int nr)

```
....
773.                syms_cache->data = calloc(nr, sizeof(*syms_cache-
>data));
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1354
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	827	827
Object	name	name

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int partitions__add_partition(struct partitions *partitions,

```
....
827.        partition->name = strdup(name);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1355
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	847	847
Object	partitions	partitions

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
847.        partitions = calloc(1, sizeof(*partitions));
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1356

Status	New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	842	842
Object	d	d

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
842.    if ((d=opendir(dir)) == NULL) return NULL;
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1357
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	842	842
Object	d	d

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
842.    if ((d=opendir(dir)) == NULL) return NULL;
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1358
Status	New

	Source	Destination
File	jasper-software@@jasper-version-2.0.17-CVE-2022-2963-FP.c	jasper-software@@jasper-version-2.0.17-CVE-2022-2963-FP.c

Line	353	353
Object	cmdopts	cmdopts

Code Snippet
File Name jasper-software@@jasper-version-2.0.17-CVE-2022-2963-FP.c
Method cmdopts_t *cmdopts_parse(int argc, char **argv)

```
....
353.        if (!(cmdopts = malloc(sizeof(cmdopts_t)))) {
```

Memory Leak\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1359
Status New

	Source	Destination
File	jasper-software@@jasper-version-2.0.23-CVE-2022-2963-FP.c	jasper-software@@jasper-version-2.0.23-CVE-2022-2963-FP.c
Line	353	353
Object	cmdopts	cmdopts

Code Snippet
File Name jasper-software@@jasper-version-2.0.23-CVE-2022-2963-FP.c
Method cmdopts_t *cmdopts_parse(int argc, char **argv)

```
....
353.        if (!(cmdopts = malloc(sizeof(cmdopts_t)))) {
```

Memory Leak\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1360
Status New

	Source	Destination
File	jasper-software@@jasper-version-2.0.27-CVE-2022-2963-FP.c	jasper-software@@jasper-version-2.0.27-CVE-2022-2963-FP.c
Line	353	353
Object	cmdopts	cmdopts

Code Snippet
File Name jasper-software@@jasper-version-2.0.27-CVE-2022-2963-FP.c

Method	cmdopts_t *cmdopts_parse(int argc, char **argv)

```
....
353.        if (!(cmdopts = malloc(sizeof(cmdopts_t)))) {
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1361
Status	New

	Source	Destination
File	jasper-software@@jasper-version-2.0.33-CVE-2022-2963-FP.c	jasper-software@@jasper-version-2.0.33-CVE-2022-2963-FP.c
Line	353	353
Object	cmdopts	cmdopts

Code Snippet
File Name jasper-software@@jasper-version-2.0.33-CVE-2022-2963-FP.c
Method cmdopts_t *cmdopts_parse(int argc, char **argv)

```
....
353.        if (!(cmdopts = malloc(sizeof(cmdopts_t)))) {
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1362
Status	New

	Source	Destination
File	jasper-software@@jasper-version-3.0.0-CVE-2022-2963-FP.c	jasper-software@@jasper-version-3.0.0-CVE-2022-2963-FP.c
Line	441	441
Object	cmdopts	cmdopts

Code Snippet
File Name jasper-software@@jasper-version-3.0.0-CVE-2022-2963-FP.c
Method cmdopts_t *cmdopts_parse(int argc, char **argv)

```
....
441.        if (!(cmdopts = malloc(sizeof(cmdopts_t)))) {
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1363
Status	New

	Source	Destination
File	jasper-software@@jasper-version-3.0.4-CVE-2022-2963-FP.c	jasper-software@@jasper-version-3.0.4-CVE-2022-2963-FP.c
Line	441	441
Object	cmdopts	cmdopts

Code Snippet
File Name jasper-software@@jasper-version-3.0.4-CVE-2022-2963-FP.c
Method cmdopts_t *cmdopts_parse(int argc, char **argv)

```
....
441.        if (!(cmdopts = malloc(sizeof(cmdopts_t)))) {
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1364
Status	New

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	51	51
Object	tail	tail

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
51.             if ((head = tail = malloc(sizeof *head)) == NULL ||
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=455
Status	New

Calling free() (line 1553) on a variable that was not dynamically allocated (line 1553) in file ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c may result with a crash.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1565	1565
Object	link	link

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static void x509_free_chain (struct refcnt *refcnt) {

```
....
1565.             free ( link );
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=456
Status	New

Calling free() (line 1553) on a variable that was not dynamically allocated (line 1553) in file ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c may result with a crash.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1569	1569
Object	chain	chain

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method static void x509_free_chain (struct refcnt *refcnt) {

```
....
1569.       free ( chain );
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=457
Status	New

Calling free() (line 1781) on a variable that was not dynamically allocated (line 1781) in file ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c may result with a crash.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1800	1800
Object	cursor	cursor

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method int image_x509 (struct image *image, size_t offset,

```
....
1800.       free ( cursor );
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=458
Status	New

Calling free() (line 1781) on a variable that was not dynamically allocated (line 1781) in file ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c may result with a crash.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1806	1806
Object	cursor	cursor

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method int image_x509 (struct image *image, size_t offset,

```
....
1806.       free ( cursor );
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=459

Status	New

Calling free() (line 557) on a variable that was not dynamically allocated (line 557) in file koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	592	592
Object	context	context

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method void *window_manager_animate_window_list_thread_proc(void *data)

```
....
592.        free(context);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=460
Status	New

Calling free() (line 52) on a variable that was not dynamically allocated (line 52) in file krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c
Line	149	149
Object	realmstr	realmstr

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
149.        free(realmstr);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=461
Status	New

Calling free() (line 52) on a variable that was not dynamically allocated (line 52) in file krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c
Line	150	150
Object	ai	ai

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
150.        free(ai);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=462
Status New

Calling free() (line 1101) on a variable that was not dynamically allocated (line 1101) in file krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c
Line	1137	1137
Object	stype	stype

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c
Method is_referral_req(kdc_realm_t *kdc_active_realm, krb5_kdc_req *request)

```
....
1137.       free(stype);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=463
Status New

Calling free() (line 1146) on a variable that was not dynamically allocated (line 1146) in file krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c
Line	1182	1182
Object	hostname	hostname

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2021-37750-TP.c
Method find_referral_tgs(kdc_realm_t *kdc_active_realm, krb5_kdc_req *request,

```
....
1182.       free(hostname);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=464
Status New

Calling free() (line 454) on a variable that was not dynamically allocated (line 454) in file krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Line	476	476
Object	pac_princname	pac_princname

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Method k5_pac_validate_client(krb5_context context,

```
....
476.           free(pac_princname);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=465
Status New

Calling free() (line 454) on a variable that was not dynamically allocated (line 454) in file krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Line	483	483
Object	pac_princname	pac_princname

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Method k5_pac_validate_client(krb5_context context,

```
....
483.        free(pac_princname);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=466
Status New

Calling free() (line 840) on a variable that was not dynamically allocated (line 840) in file krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Line	851	851
Object	pacctx	pacctx

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Method mspac_request_fini(krb5_context kcontext,

```
....
851.            free(pacctx);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=467
Status New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Line	1078	1078
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1078.       if (p) free(p);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=468
Status New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Line	1088	1088
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1088.           free(p);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=469
Status New

Calling free() (line 66) on a variable that was not dynamically allocated (line 66) in file krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	73	73
Object	cur	cur

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method free_mkey_list(krb5_context context, krb5_keylist_node *mkey_list)

```
....
73.           free(cur);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=470
Status New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	143	143
Object	prev	prev

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_dbe_free_key_list(krb5_context context, krb5_keylist_node *val)

```
....
143.           free(prev);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=471
Status New

Calling free() (line 859) on a variable that was not dynamically allocated (line 859) in file krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	905	905
Object	curr	curr

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
905.                free(curr);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=472
Status New

Calling free() (line 996) on a variable that was not dynamically allocated (line 996) in file krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1016	1016
Object	princ_name	princ_name

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1016.       free(princ_name);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=473
Status New

Calling free() (line 1435) on a variable that was not dynamically allocated (line 1435) in file krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1453	1453
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1453.           free(fname);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=474
Status New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1567	1567
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1567.           free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=475
Status New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1583	1583
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1583.       free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=476
Status New

Calling free() (line 52) on a variable that was not dynamically allocated (line 52) in file krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c
Line	149	149
Object	realmstr	realmstr

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
149.       free(realmstr);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=477
Status New

Calling free() (line 52) on a variable that was not dynamically allocated (line 52) in file krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c
Line	150	150
Object	ai	ai

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
150.        free(ai);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=478
Status New

Calling free() (line 1101) on a variable that was not dynamically allocated (line 1101) in file krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c
Line	1137	1137
Object	stype	stype

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c
Method is_referral_req(kdc_realm_t *kdc_active_realm, krb5_kdc_req *request)

```
....
1137.       free(stype);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=479
Status New

Calling free() (line 1146) on a variable that was not dynamically allocated (line 1146) in file krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c
Line	1182	1182
Object	hostname	hostname

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2021-37750-TP.c
Method find_referral_tgs(kdc_realm_t *kdc_active_realm, krb5_kdc_req *request,

```
....
1182.       free(hostname);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=480
Status New

Calling free() (line 454) on a variable that was not dynamically allocated (line 454) in file krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Line	476	476
Object	pac_princname	pac_princname

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Method k5_pac_validate_client(krb5_context context,

```
....
476.           free(pac_princname);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=481
Status New

Calling free() (line 454) on a variable that was not dynamically allocated (line 454) in file krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Line	483	483
Object	pac_princname	pac_princname

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Method k5_pac_validate_client(krb5_context context,

```
....
483.        free(pac_princname);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=482
Status New

Calling free() (line 840) on a variable that was not dynamically allocated (line 840) in file krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Line	851	851
Object	pacctx	pacctx

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Method mspac_request_fini(krb5_context kcontext,

```
....
851.            free(pacctx);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=483
Status New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Line	1078	1078
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1078.       if (p) free(p);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=484
Status New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Line	1088	1088
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1088.            free(p);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=485
Status New

Calling free() (line 66) on a variable that was not dynamically allocated (line 66) in file krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	73	73
Object	cur	cur

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method free_mkey_list(krb5_context context, krb5_keylist_node *mkey_list)

```
....
73.           free(cur);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=486
Status New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	143	143
Object	prev	prev

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_free_key_list(krb5_context context, krb5_keylist_node *val)

```
....
143.           free(prev);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=487
Status New

Calling free() (line 859) on a variable that was not dynamically allocated (line 859) in file krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	905	905
Object	curr	curr

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
905.                free(curr);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=488
Status New

Calling free() (line 996) on a variable that was not dynamically allocated (line 996) in file krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1016	1016
Object	princ_name	princ_name

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1016.       free(princ_name);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=489
Status New

Calling free() (line 1435) on a variable that was not dynamically allocated (line 1435) in file krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1453	1453
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1453.           free(fname);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=490
Status New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1567	1567
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1567.           free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=491
Status New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1583	1583
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1583.       free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=492
Status New

Calling free() (line 454) on a variable that was not dynamically allocated (line 454) in file krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Line	476	476
Object	pac_princname	pac_princname

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Method k5_pac_validate_client(krb5_context context,

```
....
476.            free(pac_princname);
```

MemoryFree on StackVariable\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=493
Status New

Calling free() (line 454) on a variable that was not dynamically allocated (line 454) in file krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Line	483	483
Object	pac_princname	pac_princname

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Method k5_pac_validate_client(krb5_context context,

```
....
483.        free(pac_princname);
```

MemoryFree on StackVariable\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=494
Status New

Calling free() (line 840) on a variable that was not dynamically allocated (line 840) in file krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Line	851	851
Object	pacctx	pacctx

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Method mspac_request_fini(krb5_context kcontext,

```
....
851.            free(pacctx);
```

MemoryFree on StackVariable\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=495
Status New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Line	1078	1078
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1078.       if (p) free(p);
```

MemoryFree on StackVariable\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=496
Status New

Calling free() (line 1056) on a variable that was not dynamically allocated (line 1056) in file krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Line	1088	1088
Object	p	p

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Method xdr_krb5_principal(XDR *xdrs, krb5_principal *objp)

```
....
1088.            free(p);
```

MemoryFree on StackVariable\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=497
Status New

Calling free() (line 66) on a variable that was not dynamically allocated (line 66) in file krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	73	73
Object	cur	cur

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method free_mkey_list(krb5_context context, krb5_keylist_node *mkey_list)

```
....
73.           free(cur);
```

MemoryFree on StackVariable\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=498
Status New

Calling free() (line 135) on a variable that was not dynamically allocated (line 135) in file krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	143	143
Object	prev	prev

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_dbe_free_key_list(krb5_context context, krb5_keylist_node *val)

```
....
143.           free(prev);
```

MemoryFree on StackVariable\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=499
Status New

Calling free() (line 859) on a variable that was not dynamically allocated (line 859) in file krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	905	905
Object	curr	curr

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
905.                free(curr);
```

MemoryFree on StackVariable\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=500
Status New

Calling free() (line 996) on a variable that was not dynamically allocated (line 996) in file krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1016	1016
Object	princ_name	princ_name

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_delete_principal(krb5_context kcontext, krb5_principal search_for)

```
....
1016.       free(princ_name);
```

MemoryFree on StackVariable\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=501
Status New

Calling free() (line 1435) on a variable that was not dynamically allocated (line 1435) in file krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1453	1453
Object	fname	fname

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_setup_mkey_name(krb5_context context, const char *keyname,

```
....
1453.           free(fname);
```

MemoryFree on StackVariable\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=502
Status New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1567	1567
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1567.           free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=503
Status New

Calling free() (line 1549) on a variable that was not dynamically allocated (line 1549) in file krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1583	1583
Object	unparse_mod_princ	unparse_mod_princ

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_dbe_update_mod_princ_data(krb5_context context, krb5_db_entry *entry,

```
....
1583.       free(unparse_mod_princ);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=504
Status	New

Calling free() (line 52) on a variable that was not dynamically allocated (line 52) in file krb5@@krb5-krb5-1.19.1-final-CVE-2021-36222-TP.c may result with a crash.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2021-36222-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2021-36222-TP.c
Line	149	149
Object	realmstr	realmstr

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2021-36222-TP.c
Method ec_verify(krb5_context context, krb5_data *req_pkt, krb5_kdc_req *request,

```
....
149.       free(realmstr);
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0
Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=535
Status	New

The function der_len in krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c at line 631 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	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Line	639	639
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
639.        der = malloc(der_len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=536
Status	New

The function der_len in krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c at line 633 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	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Line	641	641
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
641.        der = malloc(der_len);
```

Wrong Size t Allocation\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=537
Status	New

The function der_len in krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c at line 633 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	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Line	641	641
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
641.      der = malloc(der_len);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=538
Status	New

The function der_len in krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c at line 620 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	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Line	628	628
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.      der = malloc(der_len);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=539
Status	New

The function der_len in krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c at line 620 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	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Line	628	628
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.      der = malloc(der_len);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=540
Status	New

The function der_len in krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c at line 620 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	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Line	628	628
Object	der_len	der_len

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Method store_der(const taginfo *t, const uint8_t *asn1, size_t len, void *val,

```
....
628.      der = malloc(der_len);
```

Wrong Size t Allocation\Path 7:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=541
Status	New

The function new_cap in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 48 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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	60	60
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
60.         tmp = realloc(ksyms->strs, new_cap);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=542
Status	New

The function new_cap in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 46 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	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	58	58
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
58.         tmp = realloc(ksyms->strs, new_cap);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=543
Status	New

The function new_cap in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 46 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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	58	58
Object	new_cap	new_cap

Code Snippet

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
58.         tmp = realloc(ksyms->strs, new_cap);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=544
Status	New

The function new_cap in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 47 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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	59	59
Object	new_cap	new_cap

Code Snippet

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
59.         tmp = realloc(ksyms->strs, new_cap);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=545
Status	New

The function new_cap in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 48 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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	60	60
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
60.         tmp = realloc(ksyms->strs, new_cap);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=546
Status	New

The function len in krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c at line 294 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	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Line	358	358
Object	len	len

Code Snippet

File Name	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Method	krb5_pac_parse(krb5_context context,

```
....
358.      pac->data.data = realloc(pac->data.data, len);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=547
Status	New

The function len in krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c at line 294 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	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Line	358	358
Object	len	len

Code Snippet

File Name	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Method	krb5_pac_parse(krb5_context context,

```
....
358.      pac->data.data = realloc(pac->data.data, len);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=548
Status	New

The function len in krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c at line 294 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	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Line	358	358
Object	len	len

Code Snippet	
File Name	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Method	krb5_pac_parse(krb5_context context,

```
....
358.      pac->data.data = realloc(pac->data.data, len);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=549
Status	New

The function len in krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c at line 294 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	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Line	358	358
Object	len	len

Code Snippet	
File Name	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Method	krb5_pac_parse(krb5_context context,

```
....
358.      pac->data.data = realloc(pac->data.data, len);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=550
Status	New

The function len in krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c at line 294 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	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Line	358	358
Object	len	len

Code Snippet	
File Name	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Method	krb5_pac_parse(krb5_context context,

```
....
358.      pac->data.data = realloc(pac->data.data, len);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=551
Status	New

The function new_cap in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 48 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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	70	70
Object	new_cap	new_cap

Code Snippet	
File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
70.          tmp = realloc(ksyms->syms, sizeof(*ksyms->syms) * new_cap);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=552
Status	New

The function new_cap in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 407 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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	423	423

Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int dso__add_sym(struct dso *dso, const char *name, uint64_t start,

```
....
423.              tmp = realloc(dso->syms, sizeof(*dso->syms) *
new_cap);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=553
Status	New

The function new_cap in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 46 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	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	68	68
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
68.          tmp = realloc(ksyms->syms, sizeof(*ksyms->syms) * new_cap);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=554
Status	New

The function new_cap in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 397 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	iovisor@@bcc-v0.21.0-CVE-2021-3520-	iovisor@@bcc-v0.21.0-CVE-2021-3520-

	FP.c	FP.c
Line	413	413
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int dso__add_sym(struct dso *dso, const char *name, uint64_t start,

```
....
413.              tmp = realloc(dso->syms, sizeof(*dso->syms) *
new_cap);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=555
Status	New

The function new_cap in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 46 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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	68	68
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
68.         tmp = realloc(ksyms->syms, sizeof(*ksyms->syms) * new_cap);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=556
Status	New

The function new_cap in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 397 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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	413	413
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int dso__add_sym(struct dso *dso, const char *name, uint64_t start,

```
....
413.              tmp = realloc(dso->syms, sizeof(*dso->syms) *
new_cap);
```

Wrong Size t Allocation\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=557
Status New

The function new_cap in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 47 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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	69	69
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
69.          tmp = realloc(ksyms->syms, sizeof(*ksyms->syms) * new_cap);
```

Wrong Size t Allocation\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=558
Status New

The function new_cap in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 398 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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	414	414
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int dso__add_sym(struct dso *dso, const char *name, uint64_t start,

```
....
414.                tmp = realloc(dso->syms, sizeof(*dso->syms) *
new_cap);
```

Wrong Size t Allocation\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=559
Status New

The function new_cap in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 48 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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	70	70
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int ksyms__add_symbol(struct ksyms *ksyms, const char *name, unsigned long addr)

```
....
70.         tmp = realloc(ksyms->syms, sizeof(*ksyms->syms) * new_cap);
```

Wrong Size t Allocation\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=560
Status	New

The function new_cap in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 407 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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	423	423
Object	new_cap	new_cap

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int dso__add_sym(struct dso *dso, const char *name, uint64_t start,

```
....
423.              tmp = realloc(dso->syms, sizeof(*dso->syms) *
new_cap);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=561
Status	New

The function pad in krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c at line 36 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	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Line	68	68
Object	pad	pad

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Method k5_pac_add_buffer(krb5_context context,

```
....
68.                          pac->data.length + PAC_INFO_BUFFER_LENGTH +
data->length + pad);
```

Wrong Size t Allocation\Path 28:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=562
Status	New

The function pad in krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c at line 36 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	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Line	68	68
Object	pad	pad

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Method k5_pac_add_buffer(krb5_context context,

```
....
68.                         pac->data.length + PAC_INFO_BUFFER_LENGTH +
data->length + pad);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=563
Status	New

The function pad in krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c at line 36 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	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Line	68	68
Object	pad	pad

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Method k5_pac_add_buffer(krb5_context context,

```
....
68.                         pac->data.length + PAC_INFO_BUFFER_LENGTH +
data->length + pad);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=564
Status	New

The function pad in krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c at line 36 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	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Line	68	68
Object	pad	pad

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Method k5_pac_add_buffer(krb5_context context,

```
....
68.                          pac->data.length + PAC_INFO_BUFFER_LENGTH +
data->length + pad);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=565
Status	New

The function pad in krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c at line 36 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	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Line	68	68
Object	pad	pad

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Method k5_pac_add_buffer(krb5_context context,

```
....
68.                          pac->data.length + PAC_INFO_BUFFER_LENGTH +
data->length + pad);
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=566
Status	New

The function pathsize in jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c at line 826 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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	838	838
Object	pathsize	pathsize

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
838.      path=xmalloc(pathsize = strlen(dir)+PATH_MAX);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=567
Status	New

The function pathsize in jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c at line 894 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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	947	947
Object	pathsize	pathsize

Code Snippet

File Name	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method	struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
947.    path = xmalloc(pathsize=PATH_MAX);
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=568
Status	New

The function pathsize in jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c at line 826 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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	838	838
Object	pathsize	pathsize

Code Snippet

File Name	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method	struct _info **read_dir(char *dir, int *n, int infotop)

```
....
838.      path=xmalloc(pathsize = strlen(dir)+PATH_MAX);
```

Wrong Size t Allocation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=569
Status	New

The function pathsize in jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c at line 894 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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	947	947
Object	pathsize	pathsize

Code Snippet	
File Name	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method	struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
947.    path = xmalloc(pathsize=PATH_MAX);
```

Wrong Size t Allocation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=570
Status	New

The function pathsize in jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c at line 826 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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	851	851
Object	pathsize	pathsize

Code Snippet	
File Name	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method	struct _info **read_dir(char *dir, int *n, int infotop)

```
....
851.      if (strlen(dir)+strlen(ent->d_name)+2 > pathsize) path =
xrealloc(path,pathsize=(strlen(dir)+strlen(ent->d_name)+PATH_MAX));
```

Wrong Size t Allocation\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=571
Status	New

The function pathsize in jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c at line 894 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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c

Line	972	972
Object	pathsize	pathsize

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
972.              if (strlen(d)+strlen((*dir)->lnk)+2 > pathsize)
path=xrealloc(path,pathsize=(strlen(d)+strlen((*dir)->name)+1024));
```

Wrong Size t Allocation\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=572
Status	New

The function pathsize in jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c at line 894 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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	980	980
Object	pathsize	pathsize

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
980.        if (strlen(d)+strlen((*dir)->name)+2 > pathsize)
path=xrealloc(path,pathsize=(strlen(d)+strlen((*dir)->name)+1024));
```

Wrong Size t Allocation\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=573
Status	New

The function pathsize in jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c at line 826 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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	851	851
Object	pathsize	pathsize

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
851.      if (strlen(dir)+strlen(ent->d_name)+2 > pathsize) path =
xrealloc(path,pathsize=(strlen(dir)+strlen(ent->d_name)+PATH_MAX));
```

Wrong Size t Allocation\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=574
Status New

The function pathsize in jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c at line 894 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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	972	972
Object	pathsize	pathsize

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
972.              if (strlen(d)+strlen((*dir)->lnk)+2 > pathsize)
path=xrealloc(path,pathsize=(strlen(d)+strlen((*dir)->name)+1024));
```

Wrong Size t Allocation\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=575
Status New

The function pathsize in jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c at line 894 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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	980	980
Object	pathsize	pathsize

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
980.        if (strlen(d)+strlen((*dir)->name)+2 > pathsize)
path=xrealloc(path,pathsize=(strlen(d)+strlen((*dir)->name)+1024));
```

Wrong Size t Allocation\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=576
Status New

The function count in krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c at line 1468 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	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Line	1488	1488
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Method decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1488.          newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=577
Status	New

The function count in krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c at line 1470 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	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Line	1490	1490
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Method decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1490.          newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=578
Status	New

The function count in krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c at line 1470 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	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Line	1490	1490
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Method decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1490.          newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=579
Status	New

The function count in krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c at line 1458 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	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Line	1478	1478
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Method decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1478.           newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=580
Status	New

The function count in krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c at line 1458 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	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Line	1478	1478
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Method decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1478.           newseq = realloc(seq, (count + 1) * elemtype->size);
```

Wrong Size t Allocation\Path 47:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=581
Status	New

The function count in krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c at line 1458 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	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Line	1478	1478
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Method decode_sequence_of(const uint8_t *asn1, size_t len,

```
....
1478.           newseq = realloc(seq, (count + 1) * elemtype->size);
```

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=1020038&projectid=20031&pathid=433
Status	New

The application performs an illegal operation in cvtRational, in julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c. In line 1280, the program attempts to divide by denom, 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 denom in cvtRational of julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c, at line 1280.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c
Line	1289	1289
Object	denom	denom

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c
Method cvtRational(TIFF* tif, TIFFDirEntry* dir, uint32 num, uint32 denom, float* rv)

```
....
1289.                    *rv = ((float)num / (float)denom);
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=434
Status	New

The application performs an illegal operation in cvtRational, in julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c. In line 1280, the program attempts to divide by denom, 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 denom in cvtRational of julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c, at line 1280.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c
Line	1291	1291
Object	denom	denom

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-29776-TP.c
Method cvtRational(TIFF* tif, TIFFDirEntry* dir, uint32 num, uint32 denom, float* rv)

```
....
1291.                    *rv = ((float)(int32)num / (float)(int32)denom);
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=435
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c. In line 487, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c, at line 487.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c
Line	504	504
Object	array_size	array_size

Code Snippet	
File Name	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c
Method	static bool checkreturn allocate_field(pb_istream_t *stream, void *pData, size_t data_size, size_t array_size)

```
....
504.             if (size_max / array_size < data_size)
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=436
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c. In line 487, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c, at line 487.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c
Line	504	504
Object	array_size	array_size

Code Snippet	
File Name	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c
Method	static bool checkreturn allocate_field(pb_istream_t *stream, void *pData, size_t data_size, size_t array_size)

```
....
504.             if (size_max / array_size < data_size)
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=437
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.5.1-	keepkey@@keepkey-firmware-v6.5.1-

	CVE-2020-26243-TP.c	CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=438
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=439
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=440
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=441
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=442
Status New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=443
Status New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=444
Status New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=445
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=446
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=447
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.         if (size_max / array_size < data_size) {
```

Divide By Zero\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=448
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=449
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=450
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet	
File Name	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c
Method	static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=451
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c
Line	491	491
Object	array_size	array_size

Code Snippet	
File Name	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c
Method	static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=452
Status	New

The application performs an illegal operation in allocate_field, in keepkey@@keepkey-firmware-v7.9.1-CVE-2020-5235-TP.c. In line 475, the program attempts to divide by array_size, 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 array_size in allocate_field of keepkey@@keepkey-firmware-v7.9.1-CVE-2020-5235-TP.c, at line 475.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-5235-TP.c

Line	491	491
Object	array_size	array_size

Code Snippet
File Name keepkey@@keepkey-firmware-v7.9.1-CVE-2020-5235-TP.c
Method static bool checkreturn allocate_field(pb_istream_t *stream, void *pData,

```
....
491.        if (size_max / array_size < data_size) {
```

Divide By Zero\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=453
Status	New

The application performs an illegal operation in LibarchivePlugin::extractFiles, in KDE@@ark-v21.11.80-CVE-2020-24654-TP.c. In line 180, the program attempts to divide by totalEntriesCount, 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 totalEntriesCount in LibarchivePlugin::extractFiles of KDE@@ark-v21.11.80-CVE-2020-24654-TP.c, at line 180.

	Source	Destination
File	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Line	408	408
Object	totalEntriesCount	totalEntriesCount

Code Snippet
File Name KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Method bool LibarchivePlugin::extractFiles(const QVector<Archive::Entry*> &files, const QString &destinationDirectory, const ExtractionOptions &options)

```
....
408.                    Q_EMIT progress(float(progressEntryCount) /
totalEntriesCount);
```

Divide By Zero\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=454
Status	New

The application performs an illegal operation in LibarchivePlugin::copyData, in KDE@@ark-v21.11.80-CVE-2020-24654-TP.c. In line 531, the program attempts to divide by m_extractedFilesSize, 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 m_extractedFilesSize in LibarchivePlugin::copyData of KDE@@ark-v21.11.80-CVE-2020-24654-TP.c, at line 531.

	Source	Destination
File	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Line	546	546
Object	m_extractedFilesSize	m_extractedFilesSize

Code Snippet
File Name KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Method void LibarchivePlugin::copyData(const QString& filename, struct archive *source, struct archive *dest, bool partialprogress)

```
....
546.              Q_EMIT progress(float(m_currentExtractedFilesSize) /
m_extractedFilesSize);
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description
Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2572
Status	New

The size of the buffer used by syms__add_dso in Pointer, at line 323 of iovisor@@bcc-0.29.0-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 *syms__load_file passes to buf, at line 656 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	680	343
Object	buf	Pointer

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
680.                          (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.              memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2573
Status	New

The size of the buffer used by syms__add_dso in dso, at line 323 of iovisor@@bcc-0.29.0-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 *syms__load_file passes to buf, at line 656 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	680	343
Object	buf	dso

Code Snippet

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
680.                          (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.              memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2574
Status	New

The size of the buffer used by syms__add_dso in sizeof, at line 323 of iovisor@@bcc-0.29.0-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 *syms__load_file passes to buf, at line 656 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	680	343
Object	buf	sizeof

Code Snippet

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
680.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2575
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.21.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	546	565
Object	Address	sz

Code Snippet

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
565.         memcpy(image, (void *)start_addr, sz);
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2576
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.21.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	546	565
Object	Address	sz

Code Snippet

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
565.         memcpy(image, (void *)start_addr, sz);
```

Stored Buffer Overflow boundcpy\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2577
Status	New

The size of the buffer used by syms__add_dso in Pointer, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Line	663	333
Object	buf	Pointer

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2578
Status	New

The size of the buffer used by syms__add_dso in dso, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	333
Object	buf	dso

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.              memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2579
Status	New

The size of the buffer used by syms__add_dso in sizeof, at line 313 of iovisor@@bcc-v0.21.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	663	333
Object	buf	sizeof

Code Snippet

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.              memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2580
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.23.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	546	565
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
565.         memcpy(image, (void *)start_addr, sz);
```

Stored Buffer Overflow boundcpy\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2581
Status New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.23.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	546	565
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
565.         memcpy(image, (void *)start_addr, sz);
```

Stored Buffer Overflow boundcpy\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2582
Status New

The size of the buffer used by syms__add_dso in Pointer, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	663	333
Object	buf	Pointer

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2583
Status New

The size of the buffer used by syms__add_dso in dso, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	663	333
Object	buf	dso

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
663.                        &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2584
Status	New

The size of the buffer used by syms__add_dso in sizeof, at line 313 of iovisor@@bcc-v0.23.0-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 *syms__load_file passes to buf, at line 642 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	663	333
Object	buf	sizeof

Code Snippet

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
663.                        &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
333.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2585
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 528 of iovisor@@bcc-v0.25.0-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 create_tmp_vdso_image passes to Address, at line 528 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	547	566
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
547.                            &start_addr, &end_addr, buf);
....
566.        memcpy(image, (void *)start_addr, sz);
```

Stored Buffer Overflow boundcpy\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2586
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 528 of iovisor@@bcc-v0.25.0-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 create_tmp_vdso_image passes to Address, at line 528 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	547	566
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
547.                            &start_addr, &end_addr, buf);
....
566.        memcpy(image, (void *)start_addr, sz);
```

Stored Buffer Overflow boundcpy\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2587
Status	New

The size of the buffer used by syms__add_dso in Pointer, at line 314 of iovisor@@bcc-v0.25.0-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 *syms__load_file passes to buf, at line 643 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	664	334
Object	buf	Pointer

Code Snippet

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
664.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
334.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2588
Status	New

The size of the buffer used by syms__add_dso in dso, at line 314 of iovisor@@bcc-v0.25.0-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 *syms__load_file passes to buf, at line 643 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Line	664	334
Object	buf	dso

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
664.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
334.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2589
Status	New

The size of the buffer used by syms__add_dso in sizeof, at line 314 of iovisor@@bcc-v0.25.0-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 *syms__load_file passes to buf, at line 643 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	664	334
Object	buf	sizeof

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
664.                            &map.dev_minor, &map.inode, buf);
```

File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
334.              memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2590
Status	New

The size of the buffer used by syms__add_dso in Pointer, at line 323 of iovisor@@bcc-v0.30.0-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 *syms__load_file passes to buf, at line 657 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	681	343
Object	buf	Pointer

Code Snippet

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method struct syms *syms__load_file(const char *fname)

```
....
681.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.              memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2591
Status	New

The size of the buffer used by syms__add_dso in dso, at line 323 of iovisor@@bcc-v0.30.0-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 *syms__load_file passes to buf, at line 657 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	681	343
Object	buf	dso

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
681.                            (long long*)&map.inode, buf);
```

File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.                memset(dso, 0, sizeof(*dso));
```

Stored Buffer Overflow boundcpy\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2592
Status New

The size of the buffer used by syms__add_dso in sizeof, at line 323 of iovisor@@bcc-v0.30.0-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 *syms__load_file passes to buf, at line 657 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	681	343
Object	buf	sizeof

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
681.                            (long long*)&map.inode, buf);
```

File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	static int syms__add_dso(struct syms *syms, struct map *map, const char *name)

```
....
343.              memset(dso, 0, sizeof(*dso));
```

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=1020038&projectid=20031&pathid=97
Status	New

The pointer s2 at iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c in line 89 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	95	95
Object	s2	s2

Code Snippet

File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	static int ksym_cmp(const void *p1, const void *p2)

```
....
95.   return s1->addr < s2->addr ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=98
Status	New

The pointer s2 at iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c in line 440 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	446	446
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int sym_cmp(const void *p1, const void *p2)

```
....
446.        return s1->start < s2->start ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=99
Status New

The pointer s2 at iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c in line 87 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	93	93
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int ksym_cmp(const void *p1, const void *p2)

```
....
93.   return s1->addr < s2->addr ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=100
Status New

The pointer s2 at iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c in line 429 is being used after it has been freed.

	Source	Destination

File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	435	435
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int sym_cmp(const void *p1, const void *p2)

```
....
435.        return s1->start < s2->start ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=101
Status	New

The pointer s2 at iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c in line 87 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	93	93
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int ksym_cmp(const void *p1, const void *p2)

```
....
93.   return s1->addr < s2->addr ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=102
Status	New

The pointer s2 at iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c in line 429 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-	iovisor@@bcc-v0.23.0-CVE-2021-3520-

	FP.c	FP.c
Line	435	435
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int sym_cmp(const void *p1, const void *p2)

```
....
435.        return s1->start < s2->start ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=103
Status	New

The pointer s2 at iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c in line 88 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	94	94
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int ksym_cmp(const void *p1, const void *p2)

```
....
94.   return s1->addr < s2->addr ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=104
Status	New

The pointer s2 at iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c in line 430 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Line	436	436
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int sym_cmp(const void *p1, const void *p2)

```
....
436.        return s1->start < s2->start ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=105
Status	New

The pointer s2 at iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c in line 89 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	95	95
Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int ksym_cmp(const void *p1, const void *p2)

```
....
95.   return s1->addr < s2->addr ? -1 : 1;
```

Buffer Overflow AddressOfLocalVarReturned\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=106
Status	New

The pointer s2 at iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c in line 440 is being used after it has been freed.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	446	446

Object	s2	s2

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int sym_cmp(const void *p1, const void *p2)

```
....
446.        return s1->start < s2->start ? -1 : 1;
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1308
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	785	786
Object	data	syms_cache

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method void syms_cache__free(struct syms_cache *syms_cache)

```
....
785.        free(syms_cache->data);
786.        free(syms_cache);
```

Double Free\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1309
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-	iovisor@@bcc-v0.21.0-CVE-2021-3520-

	FP.c	FP.c
Line	752	753
Object	data	syms_cache

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method void syms_cache__free(struct syms_cache *syms_cache)

```
....
752.        free(syms_cache->data);
753.        free(syms_cache);
```

Double Free\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1310
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	752	753
Object	data	syms_cache

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method void syms_cache__free(struct syms_cache *syms_cache)

```
....
752.        free(syms_cache->data);
753.        free(syms_cache);
```

Double Free\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1311
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	753	754
Object	data	syms_cache

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method void syms_cache__free(struct syms_cache *syms_cache)

```
....
753.        free(syms_cache->data);
754.        free(syms_cache);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1312
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	786	787
Object	data	syms_cache

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method void syms_cache__free(struct syms_cache *syms_cache)

```
....
786.        free(syms_cache->data);
787.        free(syms_cache);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1313
Status	New

	Source	Destination
File	KDE@@kdeconnect-kde-v1.4.1-CVE-2020-26164-TP.c	KDE@@kdeconnect-kde-v1.4.1-CVE-2020-26164-TP.c
Line	211	211
Object	receivedPacket	receivedPacket

Code Snippet
File Name KDE@@kdeconnect-kde-v1.4.1-CVE-2020-26164-TP.c
Method void LanLinkProvider::udpBroadcastReceived()

```
....
211.                delete receivedPacket;
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1314
Status	New

	Source	Destination
File	KDE@@kdeconnect-kde-v1.4.1-CVE-2020-26164-TP.c	KDE@@kdeconnect-kde-v1.4.1-CVE-2020-26164-TP.c
Line	205	217
Object	receivedPacket	receivedPacket

Code Snippet
File Name KDE@@kdeconnect-kde-v1.4.1-CVE-2020-26164-TP.c
Method void LanLinkProvider::udpBroadcastReceived()

```
....
205.                delete receivedPacket;
....
217.                delete receivedPacket;
```

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=1020038&projectid=20031&pathid=427
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-	krb5@@krb5-krb5-1.18.1-final-CVE-

	2020-28196-TP.c	2020-28196-TP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.          digit = valcopy & 0xFF;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=428
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.          digit = valcopy & 0xFF;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=429
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-	krb5@@krb5-krb5-1.18.5-final-CVE-

	2020-28196-FP.c	2020-28196-FP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.          digit = valcopy & 0xFF;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=430
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.          digit = valcopy & 0xFF;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=431
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-	krb5@@krb5-krb5-1.19.2-final-CVE-

	2020-28196-FP.c	2020-28196-FP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.          digit = valcopy & 0xFF;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=432
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 66 of krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Line	73	73
Object	AssignExpr	AssignExpr

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Method k5_asn1_encode_int(asn1buf *buf, intmax_t val)

```
....
73.          digit = valcopy & 0xFF;
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1432

Status	New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	68	586
Object	errors	errors

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int errors;

```
....
68.  int errors;
```

File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
586.    return errors ? 2 : 0;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1433
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	68	586
Object	errors	errors

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int errors;

```
....
68.  int errors;
```

File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
586.    return errors ? 2 : 0;
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1434
Status	New

	Source	Destination
File	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Line	487	628
Object	ip_ver	ip_ver

Code Snippet
File Name irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Method capture_packet_reasm_ip(capture_info_t *capinfo, const struct pcap_pkthdr *header, u_char *packet, uint32_t *size, uint32_t *caplen)

```
....
487.      uint32_t ip_ver;
....
628.      if (ip_ver == 6 && header->caplen < link_hl + sizeof(struct ip6_hdr))
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1435
Status	New

	Source	Destination
File	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Line	487	624
Object	ip_ver	ip_ver

Code Snippet
File Name irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Method capture_packet_reasm_ip(capture_info_t *capinfo, const struct pcap_pkthdr *header, u_char *packet, uint32_t *size, uint32_t *caplen)

```
....
487.      uint32_t ip_ver;
....
624.      if (ip_ver == 4 && header->caplen < link_hl + sizeof(struct
ip))
```

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=1020038&projectid=20031&pathid=1431
Status	New

The variable declared in link at ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c in line 1657 is not initialized when it is used by link at ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c in line 1657.

	Source	Destination
File	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c	ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Line	1659	1666
Object	link	link

Code Snippet
File Name ipxe@@ipxe-v1.20.1-CVE-2022-4087-TP.c
Method x509_find_subject (struct x509_chain *certs,

```
....
1659.       struct x509_link *link;
....
1666.             cert = link->cert;
```

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=1020038&projectid=20031&pathid=2593
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	850	850
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
850.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2594
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1015	1015
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1015.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2595
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	817	817
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
817.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2596
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	990	990
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
990.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2597
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	817	817

Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
817.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2598
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	990	990
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
990.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2599
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	818	818
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
818.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2600
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	981	981
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
981.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2601
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	851	851
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
851.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2602
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1016	1016
Object	fgets	fgets

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1016.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2603
Status	New

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	26	26
Object	fgets	fgets

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.      while (fgets(alias, sizeof alias, fp) != NULL) {
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2604
Status	New

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	39	39
Object	fgets	fgets

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.             if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2605
Status New

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	26	26
Object	fgets	fgets

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.     while (fgets(alias, sizeof alias, fp) != NULL) {
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2606
Status New

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	39	39

Object	fgets	fgets

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.             if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2607
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	115	115
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
115.             ret = fscanf(f, "%lx %c %s%*[^\n]\n",
```

Improper Resource Access Authorization\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2608
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	556	556
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
556.                ret = fscanf(f, "%llx-%llx %*s %*x %*x:%*x %*u%[^\n]",
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2609
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	674	674
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
674.                ret = fscanf(f, "%llx-%llx %4s %llx %llx:%llx
%llu%[^\n]",
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2610
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1118	1118
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1118.               ret = fscanf(f, "%s %s%*[^\n]\n", addr_range,
sym_name);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2611
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1138	1138
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1138.             ret = fscanf(f, "%s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2612
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1160	1160
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1160.             ret = fscanf(f, "%*x %*c %s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2613
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	113	113
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
113.              ret = fscanf(f, "%lx %c %s%*[^\n]\n",
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2614
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	545	545
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
545.              ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
```

Improper Resource Access Authorization\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2615
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	660	660

Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
660.              ret = fscanf(f, "%lx-%lx %4s %lx %lx:%lx %lu%[^\n]",
```

Improper Resource Access Authorization\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2616
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1067	1067
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1067.             ret = fscanf(f, "%s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2617
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1089	1089
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1089.               ret = fscanf(f, "%*x %*c %s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2618
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	113	113
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
113.               ret = fscanf(f, "%lx %c %s%*[^\n]\n",
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2619
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	545	545
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
545.               ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
```

Improper Resource Access Authorization\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2620
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	660	660
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
660.              ret = fscanf(f, "%lx-%lx %4s %lx %lx:%lx %lu%[^\n]",
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2621
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	1067	1067
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1067.             ret = fscanf(f, "%s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2622
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	1089	1089
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1089.             ret = fscanf(f, "%*x %*c %s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2623
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	114	114
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
114.              ret = fscanf(f, "%lx %c %s%*[^\n]\n",
```

Improper Resource Access Authorization\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2624
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	546	546

Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.              ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
```

Improper Resource Access Authorization\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2625
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	661	661
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
661.              ret = fscanf(f, "%lx-%lx %4s %lx %lx:%lx %lu%[^\n]",
```

Improper Resource Access Authorization\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2626
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1072	1072
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1072.             ret = fscanf(f, "%s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2627
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1094	1094
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1094.             ret = fscanf(f, "%*x %*c %s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2628
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	115	115
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
115.              ret = fscanf(f, "%lx %c %s%*[^\n]\n",
```

Improper Resource Access Authorization\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2629
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	556	556
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
556.                ret = fscanf(f, "%llx-%llx %*s %*x %*x:%*x %*u%[^\n]",
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2630
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	675	675
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
675.                ret = fscanf(f, "%llx-%llx %4s %llx %llx:%llx
%llu%[^\n]",
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2631
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1119	1119
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1119.             ret = fscanf(f, "%s %s%*[^\n]\n", addr_range,
sym_name);
```

Improper Resource Access Authorization\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2632
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1139	1139
Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1139.             ret = fscanf(f, "%s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2633
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1161	1161

Object	fscanf	fscanf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1161.             ret = fscanf(f, "%*x %*c %s%*[^\n]\n", sym_name);
```

Improper Resource Access Authorization\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2634
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	850	850
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
850.         while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2635
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1015	1015
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1015.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2636
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	817	817
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
817.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2637
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	990	990
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
990.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 46:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2638
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	817	817
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
817.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2639
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	990	990
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
990.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2640
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	818	818
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
818.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2641
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	981	981
Object	buf	buf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
981.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2642
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	851	851

Object	buf	buf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
851.        while (fgets(buf, sizeof(buf), f) != NULL) {
```

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=1020038&projectid=20031&pathid=2162
Status	New

The variable declared in null at jsummers@@deark-v1.5.6-CVE-2021-28856-TP.c in line 366 is not initialized when it is used by out_params at jsummers@@deark-v1.5.6-CVE-2021-28856-TP.c in line 314.

	Source	Destination
File	jsummers@@deark-v1.5.6-CVE-2021-28856-TP.c	jsummers@@deark-v1.5.6-CVE-2021-28856-TP.c
Line	369	348
Object	null	out_params

Code Snippet
File Name jsummers@@deark-v1.5.6-CVE-2021-28856-TP.c
Method }

```
....
369.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.5.6-CVE-2021-28856-TP.c
Method {

```
....
348.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2163
Status	New

The variable declared in null at jsummers@@deark-v1.5.7-CVE-2021-28856-TP.c in line 366 is not initialized when it is used by out_params at jsummers@@deark-v1.5.7-CVE-2021-28856-TP.c in line 314.

	Source	Destination
File	jsummers@@deark-v1.5.7-CVE-2021-28856-TP.c	jsummers@@deark-v1.5.7-CVE-2021-28856-TP.c
Line	369	348
Object	null	out_params

Code Snippet

File Name jsummers@@deark-v1.5.7-CVE-2021-28856-TP.c

Method }

```
....
369.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.5.7-CVE-2021-28856-TP.c

Method {

```
....
348.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2164
Status	New

The variable declared in null at jsummers@@deark-v1.5.8-CVE-2021-28856-TP.c in line 366 is not initialized when it is used by out_params at jsummers@@deark-v1.5.8-CVE-2021-28856-TP.c in line 314.

	Source	Destination
File	jsummers@@deark-v1.5.8-CVE-2021-28856-TP.c	jsummers@@deark-v1.5.8-CVE-2021-28856-TP.c
Line	369	348
Object	null	out_params

Code Snippet
File Name jsummers@@deark-v1.5.8-CVE-2021-28856-TP.c
Method }

```
....
369.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.5.8-CVE-2021-28856-TP.c

Method {

```
....
348.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2165
Status	New

The variable declared in null at jsummers@@deark-v1.5.9-CVE-2021-28856-TP.c in line 366 is not initialized when it is used by out_params at jsummers@@deark-v1.5.9-CVE-2021-28856-TP.c in line 314.

	Source	Destination
File	jsummers@@deark-v1.5.9-CVE-2021-28856-TP.c	jsummers@@deark-v1.5.9-CVE-2021-28856-TP.c
Line	369	348
Object	null	out_params

Code Snippet
File Name jsummers@@deark-v1.5.9-CVE-2021-28856-TP.c
Method }

```
....
369.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.5.9-CVE-2021-28856-TP.c

Method {

```
....
348.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2166
Status	New

The variable declared in null at jsummers@@deark-v1.6.0-CVE-2021-28856-TP.c in line 366 is not initialized when it is used by out_params at jsummers@@deark-v1.6.0-CVE-2021-28856-TP.c in line 314.

	Source	Destination
File	jsummers@@deark-v1.6.0-CVE-2021-28856-TP.c	jsummers@@deark-v1.6.0-CVE-2021-28856-TP.c
Line	369	348
Object	null	out_params

Code Snippet

File Name jsummers@@deark-v1.6.0-CVE-2021-28856-TP.c

Method }

```
....
369.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.6.0-CVE-2021-28856-TP.c

Method {

```
....
348.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2167
Status	New

The variable declared in null at jsummers@@deark-v1.6.1-CVE-2021-28856-TP.c in line 374 is not initialized when it is used by out_params at jsummers@@deark-v1.6.1-CVE-2021-28856-TP.c in line 322.

	Source	Destination
File	jsummers@@deark-v1.6.1-CVE-2021-28856-TP.c	jsummers@@deark-v1.6.1-CVE-2021-28856-TP.c
Line	377	356
Object	null	out_params

Code Snippet

File Name jsummers@@deark-v1.6.1-CVE-2021-28856-TP.c
Method }

```
....
377.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.6.1-CVE-2021-28856-TP.c
Method {

```
....
356.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2168
Status	New

The variable declared in null at jsummers@@deark-v1.6.3-CVE-2021-28856-TP.c in line 376 is not initialized when it is used by out_params at jsummers@@deark-v1.6.3-CVE-2021-28856-TP.c in line 324.

	Source	Destination
File	jsummers@@deark-v1.6.3-CVE-2021-28856-TP.c	jsummers@@deark-v1.6.3-CVE-2021-28856-TP.c
Line	379	358
Object	null	out_params

Code Snippet
File Name jsummers@@deark-v1.6.3-CVE-2021-28856-TP.c
Method }

```
....
379.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.6.3-CVE-2021-28856-TP.c
Method {

```
....
358.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2169
Status	New

The variable declared in null at jsummers@@deark-v1.6.4-CVE-2021-28856-TP.c in line 376 is not initialized when it is used by out_params at jsummers@@deark-v1.6.4-CVE-2021-28856-TP.c in line 324.

	Source	Destination
File	jsummers@@deark-v1.6.4-CVE-2021-28856-TP.c	jsummers@@deark-v1.6.4-CVE-2021-28856-TP.c
Line	379	358
Object	null	out_params

Code Snippet
File Name jsummers@@deark-v1.6.4-CVE-2021-28856-TP.c
Method }

```
....
379.  //  0 = default behavior (currently: decode unless -opt
extractplist was used)
```

File Name jsummers@@deark-v1.6.4-CVE-2021-28856-TP.c
Method {

```
....
358.                    *oparams = mparams->out_params; // struct copy
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2170
Status	New

The variable declared in null at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c in line 1082.

	Source	Destination
File	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c
Line	1109	1114
Object	null	trailerDictionary

Code Snippet
File Name julianhille@@MuhammaraJS-1.0.0-rc.1-CVE-2022-25892-TP.c

Method	EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                    PDFDictionary* trailerDictionary = NULL;
....
1114.                    bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2171
Status	New

The variable declared in null at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c in line 1082.

	Source	Destination
File	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Line	1109	1114
Object	null	trailerDictionary

Code Snippet	
File Name	julianhille@@MuhammaraJS-1.4.0-CVE-2022-25892-TP.c
Method	EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                    PDFDictionary* trailerDictionary = NULL;
....
1114.                    bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2172
Status	New

The variable declared in null at julianhille@@MuhammaraJS-1.6.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-1.6.0-CVE-2022-25892-TP.c in line 1082.

	Source	Destination

File	julianhille@@MuhammaraJS-1.6.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.6.0-CVE-2022-25892-TP.c
Line	1109	1114
Object	null	trailerDictionary

Code Snippet
File Name julianhille@@MuhammaraJS-1.6.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
....
1114.                   bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2173
Status	New

The variable declared in null at julianhille@@MuhammaraJS-1.8.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-1.8.0-CVE-2022-25892-TP.c in line 1082.

	Source	Destination
File	julianhille@@MuhammaraJS-1.8.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-1.8.0-CVE-2022-25892-TP.c
Line	1109	1114
Object	null	trailerDictionary

Code Snippet
File Name julianhille@@MuhammaraJS-1.8.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
....
1114.                   bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2174
Status	New

The variable declared in null at julianhille@@MuhammaraJS-2.0.0-CVE-2022-25892-TP.c in line 1082 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-2.0.0-CVE-2022-25892-TP.c in line 1082.

	Source	Destination
File	julianhille@@MuhammaraJS-2.0.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-2.0.0-CVE-2022-25892-TP.c
Line	1109	1114
Object	null	trailerDictionary

Code Snippet
File Name julianhille@@MuhammaraJS-2.0.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1109.                   PDFDictionary* trailerDictionary = NULL;
....
1114.                   bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2175
Status	New

The variable declared in null at julianhille@@MuhammaraJS-2.2.0-CVE-2022-25892-TP.c in line 1083 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-2.2.0-CVE-2022-25892-TP.c in line 1083.

	Source	Destination
File	julianhille@@MuhammaraJS-2.2.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-2.2.0-CVE-2022-25892-TP.c
Line	1110	1115
Object	null	trailerDictionary

Code Snippet
File Name julianhille@@MuhammaraJS-2.2.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1110.                   PDFDictionary* trailerDictionary = NULL;
....
1115.                   bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2176
Status	New

The variable declared in null at julianhille@@MuhammaraJS-2.4.0-CVE-2022-25892-TP.c in line 1083 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-2.4.0-CVE-2022-25892-TP.c in line 1083.

	Source	Destination
File	julianhille@@MuhammaraJS-2.4.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-2.4.0-CVE-2022-25892-TP.c
Line	1110	1115
Object	null	trailerDictionary

Code Snippet
File Name julianhille@@MuhammaraJS-2.4.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1110.                   PDFDictionary* trailerDictionary = NULL;
....
1115.                   bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2177
Status	New

The variable declared in null at julianhille@@MuhammaraJS-3.1.0-CVE-2022-25892-TP.c in line 1083 is not initialized when it is used by trailerDictionary at julianhille@@MuhammaraJS-3.1.0-CVE-2022-25892-TP.c in line 1083.

	Source	Destination
File	julianhille@@MuhammaraJS-3.1.0-CVE-2022-25892-TP.c	julianhille@@MuhammaraJS-3.1.0-CVE-2022-25892-TP.c

Line	1110	1115
Object	null	trailerDictionary

Code Snippet
File Name julianhille@@MuhammaraJS-3.1.0-CVE-2022-25892-TP.c
Method EStatusCode PDFParser::ParsePreviousFileDirectory(LongFilePositionType inXrefPosition,

```
....
1110.                   PDFDictionary* trailerDictionary = NULL;
....
1115.                   bool hasPrev = trailerDictionary-
>Exists("Prev");
```

NULL Pointer Dereference\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2178
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c in line 822 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c in line 822.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c
Line	879	879
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter)

```
....
879.          *(void**)iter->pData = NULL;
```

NULL Pointer Dereference\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2179
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c in line 1140 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c in line 1140.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c
Line	1227	1227
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.4.0-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter)

```
....
1227.           *(void**)iter->pData = NULL;
```

NULL Pointer Dereference\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2180
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c in line 822 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c in line 822.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c
Line	879	879
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter)

```
....
879.           *(void**)iter->pData = NULL;
```

NULL Pointer Dereference\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2181
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c in line 1140 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c in line 1140.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c
Line	1227	1227
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.4.0-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter)

```
....
1227.           *(void**)iter->pData = NULL;
```

NULL Pointer Dereference\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2182
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2183
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.5.1-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2184
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2185
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.5.1-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2186
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2187
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.7.0-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2188
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2189
Status New

The variable declared in null at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v6.7.0-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2190
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2191
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.1.4-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2192
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2193
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.1.4-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2194
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2195
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.2.1-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2196
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2197
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.2.1-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2198
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2199
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.4.0-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2200
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2201
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.4.0-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2202
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2203
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.5.0-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2204
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2205
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.5.0-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2206
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2207
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.7.0-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2208
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2209
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c	keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.7.0-CVE-2020-5235-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2210
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c in line 778 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c in line 778.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c
Line	820	820
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c
Method static void pb_field_set_to_default(pb_field_iter_t *iter) {

```
....
820.       *(void **)iter->pData = NULL;
```

NULL Pointer Dereference\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2211
Status New

The variable declared in null at keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c in line 1057 is not initialized when it is used by Pointer at keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c in line 1057.

	Source	Destination
File	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c	keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c
Line	1130	1130
Object	null	Pointer

Code Snippet
File Name keepkey@@keepkey-firmware-v7.9.1-CVE-2020-26243-TP.c
Method static void pb_release_single_field(const pb_field_iter_t *iter) {

```
....
1130.       *(void **)iter->pData = NULL;
```

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=1020038&projectid=20031&pathid=1927
Status	New

The create_tmp_vdso_image method calls the snprintf function, at line 538 of iovisor@@bcc-0.29.0-CVE-2021-3520-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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	550	550
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
550.        snprintf(tmpfile, sizeof(tmpfile), "/proc/%ld/maps", pid);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1928
Status	New

The create_tmp_vdso_image method calls the snprintf function, at line 538 of iovisor@@bcc-0.29.0-CVE-2021-3520-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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	579	579
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
579.        snprintf(tmpfile, sizeof(tmpfile),
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1929
Status	New

The *syms__load_pid method calls the snprintf function, at line 708 of iovisor@@bcc-0.29.0-CVE-2021-3520-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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	712	712
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_pid(pid_t tgid)

```
....
712.        snprintf(fname, sizeof(fname), "/proc/%ld/maps",
(long)tgid);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1930
Status	New

The tracepoint_exists method calls the snprintf function, at line 1177 of iovisor@@bcc-0.29.0-CVE-2021-3520-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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1181	1181
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool tracepoint_exists(const char *category, const char *event)

```
....
1181.       snprintf(path, sizeof(path), "%s/events/%s/%s/format",
tracefs_path(), category, event);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1931
Status	New

The module_btf_exists method calls the snprintf function, at line 1201 of iovisor@@bcc-0.29.0-CVE-2021-3520-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	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1206	1206
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool module_btf_exists(const char *mod)

```
....
1206.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1932
Status	New

The module_btf_exists method calls the snprintf function, at line 1113 of iovisor@@bcc-v0.21.0-CVE-2021-3520-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	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1118	1118
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool module_btf_exists(const char *mod)

```
....
1118.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1933
Status	New

The create_tmp_vdso_image method calls the snprintf function, at line 527 of iovisor@@bcc-v0.21.0-CVE-2021-3520-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	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	539	539
Object	snprintf	snprintf

Code Snippet	
File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
539.        snprintf(tmpfile, sizeof(tmpfile), "/proc/%ld/maps", pid);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1934
Status	New

The create_tmp_vdso_image method calls the snprintf function, at line 527 of iovisor@@bcc-v0.21.0-CVE-2021-3520-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	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	567	567
Object	snprintf	snprintf

Code Snippet	
File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
567.        snprintf(tmpfile, sizeof(tmpfile),
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1935
Status	New

The *syms__load_pid method calls the snprintf function, at line 691 of iovisor@@bcc-v0.21.0-CVE-2021-3520-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	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	695	695
Object	snprintf	snprintf

Code Snippet	
File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	struct syms *syms__load_pid(pid_t tgid)

```
....
695.         snprintf(fname, sizeof(fname), "/proc/%ld/maps",
(long)tgid);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1936
Status	New

The fentry_exists method calls the snprintf function, at line 1003 of iovisor@@bcc-v0.21.0-CVE-2021-3520-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	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1019	1019
Object	snprintf	snprintf

Code Snippet	
File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	bool fentry_exists(const char *name, const char *mod)

```
....
1019.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1937
Status	New

The module_btf_exists method calls the snprintf function, at line 1113 of iovisor@@bcc-v0.23.0-CVE-2021-3520-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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c

Line	1118	1118
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool module_btf_exists(const char *mod)

```
....
1118.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1938
Status New

The create_tmp_vdso_image method calls the snprintf function, at line 527 of iovisor@@bcc-v0.23.0-CVE-2021-3520-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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	539	539
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
539.        snprintf(tmpfile, sizeof(tmpfile), "/proc/%ld/maps", pid);
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1939
Status New

The create_tmp_vdso_image method calls the snprintf function, at line 527 of iovisor@@bcc-v0.23.0-CVE-2021-3520-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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	567	567
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
567.        snprintf(tmpfile, sizeof(tmpfile),
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1940
Status	New

The *syms__load_pid method calls the snprintf function, at line 691 of iovisor@@bcc-v0.23.0-CVE-2021-3520-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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	695	695
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_pid(pid_t tgid)

```
....
695.        snprintf(fname, sizeof(fname), "/proc/%ld/maps",
(long)tgid);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1941
Status	New

The fentry_exists method calls the snprintf function, at line 1003 of iovisor@@bcc-v0.23.0-CVE-2021-3520-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	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	1019	1019
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool fentry_exists(const char *name, const char *mod)

```
....
1019.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1942
Status New

The module_btf_exists method calls the snprintf function, at line 1118 of iovisor@@bcc-v0.25.0-CVE-2021-3520-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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1123	1123
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool module_btf_exists(const char *mod)

```
....
1123.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1943
Status New

The create_tmp_vdso_image method calls the snprintf function, at line 528 of iovisor@@bcc-v0.25.0-CVE-2021-3520-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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	540	540
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
540.        snprintf(tmpfile, sizeof(tmpfile), "/proc/%ld/maps", pid);
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1944
Status New

The create_tmp_vdso_image method calls the snprintf function, at line 528 of iovisor@@bcc-v0.25.0-CVE-2021-3520-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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	568	568
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
568.        snprintf(tmpfile, sizeof(tmpfile),
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1945
Status New

The *syms__load_pid method calls the snprintf function, at line 692 of iovisor@@bcc-v0.25.0-CVE-2021-3520-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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	696	696
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_pid(pid_t tgid)

```
....
696.         snprintf(fname, sizeof(fname), "/proc/%ld/maps",
(long)tgid);
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1946
Status New

The fentry_can_attach method calls the snprintf function, at line 1024 of iovisor@@bcc-v0.25.0-CVE-2021-3520-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	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1039	1039
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool fentry_can_attach(const char *name, const char *mod)

```
....
1039.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 21:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1947
Status	New

The create_tmp_vdso_image method calls the snprintf function, at line 538 of iovisor@@bcc-v0.30.0-CVE-2021-3520-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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	550	550
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
550.        snprintf(tmpfile, sizeof(tmpfile), "/proc/%ld/maps", pid);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1948
Status	New

The create_tmp_vdso_image method calls the snprintf function, at line 538 of iovisor@@bcc-v0.30.0-CVE-2021-3520-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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	579	579
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
579.        snprintf(tmpfile, sizeof(tmpfile),
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1949
Status	New

The *syms__load_pid method calls the snprintf function, at line 709 of iovisor@@bcc-v0.30.0-CVE-2021-3520-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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	713	713
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_pid(pid_t tgid)

```
....
713.        snprintf(fname, sizeof(fname), "/proc/%ld/maps",
(long)tgid);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1950
Status	New

The tracepoint_exists method calls the snprintf function, at line 1178 of iovisor@@bcc-v0.30.0-CVE-2021-3520-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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1182	1182
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool tracepoint_exists(const char *category, const char *event)

```
....
1182.       snprintf(path, sizeof(path), "%s/events/%s/%s/format",
tracefs_path(), category, event);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1951
Status	New

The module_btf_exists method calls the snprintf function, at line 1202 of iovisor@@bcc-v0.30.0-CVE-2021-3520-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	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1207	1207
Object	snprintf	snprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool module_btf_exists(const char *mod)

```
....
1207.             snprintf(sysfs_mod, sizeof(sysfs_mod),
"/sys/kernel/btf/%s", mod);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1952
Status	New

The *fillinfo method calls the sprintf function, at line 1438 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	1460	1460
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method char *fillinfo(char *buf, struct _info *ent)

```
....
1460.         sprintf(buf+n, "]");
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1953
Status	New

The main method calls the snprintf function, at line 137 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	572	572
Object	snprintf	snprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
572.       snprintf(path, PATH_MAX, "%s/info/exclude", stmp);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1954
Status	New

The print_version method calls the sprintf function, at line 589 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	593	593
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c

Method	void print_version(int nl)

```
....
593.    sprintf(buf, "%.*s%s", (int)strlen(v)-2, v, nl?"\n":"");
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1955
Status	New

The **read_dir method calls the sprintf function, at line 826 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	852	852
Object	sprintf	sprintf

Code Snippet	
File Name	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method	struct _info **read_dir(char *dir, int *n, int infotop)

```
....
852.      if (es) sprintf(path, "%s%s", dir, ent->d_name);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1956
Status	New

The **read_dir method calls the sprintf function, at line 826 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	853	853
Object	sprintf	sprintf

Code Snippet

File Name	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method	struct _info **read_dir(char *dir, int *n, int infotop)

```
....
853.      else sprintf(path,"%s/%s",dir,ent->d_name);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1957
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	950	950
Object	sprintf	sprintf

Code Snippet

File Name	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method	struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
950.      sprintf(path,"%d entries exceeds filelimit, not opening
dir",n);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1958
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	973	973

Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
973.              if (fflag && !strcmp(d,"/"))
sprintf(path,"%s%s",d,(*dir)->lnk);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1959
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	974	974
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
974.              else sprintf(path,"%s/%s",d,(*dir)->lnk);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1960
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	981	981
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
981.        if (fflag && !strcmp(d,"/")) sprintf(path,"%s%s",d,(*dir)->name);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1961
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	982	982
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
982.        else sprintf(path,"%s/%s",d,(*dir)->name);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1962
Status	New

The psize method calls the sprintf function, at line 1386 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	1394	1394
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int psize(char *buf, off_t size)

```
....
1394.       if (!idx) return sprintf(buf, " %4d", (int)size);
```

Unchecked Return Value\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1963
Status New

The psize method calls the sprintf function, at line 1386 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	1395	1395
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int psize(char *buf, off_t size)

```
....
1395.       else return sprintf(buf, ((size/usize) >= 10)? " %3.0f%c" : "
%3.1f%c" , (float)size/(float)usize,unit[idx]);
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1964

Status	New

The psize method calls the sprintf function, at line 1386 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-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	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	1396	1396
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int psize(char *buf, off_t size)

```
....
1396.     } else return sprintf(buf, sizeof(off_t) == sizeof(long long)?
" %11lld" : " %9lld", (long long int)size);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1965
Status	New

The *fillinfo method calls the sprintf function, at line 1438 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	1460	1460
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method char *fillinfo(char *buf, struct _info *ent)

```
....
1460.         sprintf(buf+n, "]");
```

Unchecked Return Value\Path 40:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1966
Status	New

The main method calls the snprintf function, at line 137 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	572	572
Object	snprintf	snprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
572.      snprintf(path, PATH_MAX, "%s/info/exclude", stmp);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1967
Status	New

The print_version method calls the sprintf function, at line 589 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	593	593
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method void print_version(int nl)

```
....
593.    sprintf(buf, "%.*s%s", (int)strlen(v)-2, v, nl?"\n":"");
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1968
Status	New

The **read_dir method calls the sprintf function, at line 826 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	852	852
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
852.      if (es) sprintf(path, "%s%s", dir, ent->d_name);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1969
Status	New

The **read_dir method calls the sprintf function, at line 826 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	853	853
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
853.      else sprintf(path,"%s/%s",dir,ent->d_name);
```

Unchecked Return Value\Path 44:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1970
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	950	950
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
950.      sprintf(path,"%d entries exceeds filelimit, not opening
dir",n);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1971
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	973	973
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
973.                if (fflag && !strcmp(d,"/"))
sprintf(path,"%s%s",d,(*dir)->lnk);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1972
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	974	974
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
974.                else sprintf(path,"%s/%s",d,(*dir)->lnk);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1973
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	981	981
Object	sprintf	sprintf

Code Snippet	
File Name	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method	struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
981.        if (fflag && !strcmp(d,"/")) sprintf(path,"%s%s",d,(*dir)->name);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1974
Status	New

The **unix_getfulltree method calls the sprintf function, at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	982	982
Object	sprintf	sprintf

Code Snippet	
File Name	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method	struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
982.        else sprintf(path,"%s/%s",d,(*dir)->name);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1975
Status	New

The psize method calls the sprintf function, at line 1386 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c

Line	1394	1394
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int psize(char *buf, off_t size)

```
....
1394.       if (!idx) return sprintf(buf, " %4d", (int)size);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1976
Status	New

The psize method calls the sprintf function, at line 1386 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-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	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	1395	1395
Object	sprintf	sprintf

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int psize(char *buf, off_t size)

```
....
1395.       else return sprintf(buf, ((size/usize) >= 10)? " %3.0f%c" : "
%3.1f%c" , (float)size/(float)usize,unit[idx]);
```

Insufficiently Protected Credentials

Query Path:
CPP\Cx\CPP Low Visibility\Insufficiently Protected Credentials Version:0

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insufficiently Protected Credentials\Path 1:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2497
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1183	1185
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1185.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2498
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1185	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1195.                                                password, &size))) {
```

Insufficiently Protected Credentials\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2499
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1183	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.      char    password[BUFSIZ];
....
1195.                                                password, &size))) {
```

Insufficiently Protected Credentials\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2500
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1195	1199
Object	password	password

Code Snippet	
File Name	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                                password, &size))) {
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2501
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1185	1199
Object	password	password

Code Snippet	
File Name	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2502
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-	krb5@@krb5-krb5-1.18.1-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1183	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2503
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2504
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being

encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2505
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.      char    password[BUFSIZ];
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2506
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2507
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2508
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2509
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1183	1185
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1185.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2510
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1185	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1195.                                           password, &size))) {
```

Insufficiently Protected Credentials\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2511
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1183	1195
Object	password	password

Code Snippet	
File Name	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1195.                                                password, &size))) {
```

Insufficiently Protected Credentials\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2512
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1195	1199
Object	password	password

Code Snippet	
File Name	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method	krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                                password, &size))) {
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2513
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-	krb5@@krb5-krb5-1.18.3-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1185	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2514
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1183	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2515
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being

encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2516
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2517
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2518
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2519
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2520
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2521
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1183	1185
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1185.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2522
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1185	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1195.                                              password, &size))) {
```

Insufficiently Protected Credentials\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2523
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1183	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.      char    password[BUFSIZ];
....
1195.                                              password, &size))) {
```

Insufficiently Protected Credentials\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2524
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-	krb5@@krb5-krb5-1.18.5-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1195	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                                password, &size))) {
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2525
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1185	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2526
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being

encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1183	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2527
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2528
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2529
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.      char    password[BUFSIZ];
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2530
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2531
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2532
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.      char    password[BUFSIZ];
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2533
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1183	1185
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1185.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2534
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1185	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1195.                                           password, &size))) {
```

Insufficiently Protected Credentials\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2535
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-	krb5@@krb5-krb5-1.19.1-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1183	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.      char    password[BUFSIZ];
....
1195.                                                password, &size))) {
```

Insufficiently Protected Credentials\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2536
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1195	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                                password, &size))) {
....
1199.          pwd.data = password;
```

Insufficiently Protected Credentials\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2537
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being

encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1185	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2538
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1183	1199
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1199.           pwd.data = password;
```

Insufficiently Protected Credentials\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2539
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2540
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2541
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2542
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1195	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1195.                                           password, &size))) {
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2543
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1185	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.      unsigned int size = sizeof(password);
....
1231.          zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2544
Status	New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	1183	1231
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1231.           zap(password, sizeof(password));        /* erase it */
```

Insufficiently Protected Credentials\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2545
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Line	1183	1185
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1183.       char    password[BUFSIZ];
....
1185.       unsigned int size = sizeof(password);
```

Insufficiently Protected Credentials\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2546
Status New

Method krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c gets a user password from the password element. This element's value then flows through the code without being encrypted and is written to the database in krb5_db_fetch_mkey at line 1177 of krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-	krb5@@krb5-krb5-1.19.2-final-CVE-

	2024-6381-TP.c	2024-6381-TP.c
Line	1185	1195
Object	password	password

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Method krb5_db_fetch_mkey(krb5_context context, krb5_principal mname,

```
....
1185.       unsigned int size = sizeof(password);
....
1195.                                                password, &size))) {
```

Unreleased Resource Leak

Query Path:
CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Unreleased Resource Leak\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2104
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	1099	1099
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_lock()

```
....
1099.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2105
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Line	1099	1099
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Method capture_lock()

```
....
1099.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2106
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c
Line	1099	1099
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c
Method capture_lock()

```
....
1099.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2107
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c
Line	1080	1080

Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c
Method capture_lock()

```
....
1080.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2108
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c
Line	1080	1080
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c
Method capture_lock()

```
....
1080.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2109
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c
Line	1080	1080
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c
Method capture_lock()

```
....
1080.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2110
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c
Line	1078	1078
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c
Method capture_lock()

```
....
1078.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2111
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c
Line	1078	1078
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c
Method capture_lock()

```
....
1078.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2112
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c
Line	1078	1078
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c
Method capture_lock()

```
....
1078.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2113
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c
Line	1099	1099
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c
Method capture_lock()

```
....
1099.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2114
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c
Line	1099	1099
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c
Method capture_lock()

```
....
1099.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2115
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c
Line	1099	1099
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c
Method capture_lock()

```
....
1099.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2116
Status New

	Source	Destination
File	irontec@@sngrep-v1.5.0-CVE-2023-31981-FP.c	irontec@@sngrep-v1.5.0-CVE-2023-31981-FP.c
Line	1171	1171

Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.5.0-CVE-2023-31981-FP.c
Method capture_lock()

```
....
1171.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2117
Status New

	Source	Destination
File	irontec@@sngrep-v1.5.0-CVE-2023-31982-FP.c	irontec@@sngrep-v1.5.0-CVE-2023-31982-FP.c
Line	1171	1171
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.5.0-CVE-2023-31982-FP.c
Method capture_lock()

```
....
1171.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2118
Status New

	Source	Destination
File	irontec@@sngrep-v1.5.0-CVE-2023-36192-FP.c	irontec@@sngrep-v1.5.0-CVE-2023-36192-FP.c
Line	1171	1171
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.5.0-CVE-2023-36192-FP.c
Method capture_lock()

```
....
1171.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2119
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Line	1245	1245
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Method capture_lock()

```
....
1245.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2120
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Line	1245	1245
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Method capture_lock()

```
....
1245.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2121
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Line	1245	1245
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Method capture_lock()

```
....
1245.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2122
Status	New

	Source	Destination
File	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Line	1258	1258
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Method capture_lock()

```
....
1258.       pthread_mutex_lock(&capture_cfg.lock);
```

Unreleased Resource Leak\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2123
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2124
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2125
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c
Line	82	82

Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2126
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2127
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2128
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2129
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 27:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2130
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2131
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2132
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2133
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2134
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c
Line	82	82

Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2135
Status New

	Source	Destination
File	irontec@@sngrep-v1.5.0-CVE-2023-31981-FP.c	irontec@@sngrep-v1.5.0-CVE-2023-31981-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.5.0-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2136
Status New

	Source	Destination
File	irontec@@sngrep-v1.5.0-CVE-2023-31982-FP.c	irontec@@sngrep-v1.5.0-CVE-2023-31982-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.5.0-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2137
Status	New

	Source	Destination
File	irontec@@sngrep-v1.5.0-CVE-2023-36192-FP.c	irontec@@sngrep-v1.5.0-CVE-2023-36192-FP.c
Line	82	82
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.5.0-CVE-2023-36192-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
82.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2138
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Line	130	130
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
130.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 36:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2139
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Line	130	130
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
130.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2140
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Line	130	130
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
130.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2141
Status	New

	Source	Destination
File	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Line	130	130
Object	attr	attr

Code Snippet
File Name irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
130.      pthread_mutexattr_init(&attr);
```

Unreleased Resource Leak\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2142
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2143
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Line	88	88

Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2144
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.10-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2145
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2146
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2147
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c	irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.7-CVE-2023-36192-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 45:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2148
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2149
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2150
Status	New

	Source	Destination
File	irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.8-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2151
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c	irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-31981-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2152
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c	irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c
Line	88	88

Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-31982-FP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

Unreleased Resource Leak\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2153
Status New

	Source	Destination
File	irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c	irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c
Line	88	88
Object	capture_cfg	capture_cfg

Code Snippet
File Name irontec@@sngrep-v1.4.9-CVE-2023-36192-TP.c
Method capture_init(size_t limit, bool rtp_capture, bool rotate, size_t pcap_buffer_size)

```
....
88.      pthread_mutex_init(&capture_cfg.lock, &attr);
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3487
Status New

The *ksyms__load method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c

Line	106	106
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
106.        f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3488
Status	New

The create_tmp_vdso_image method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
551.        f = fopen(tmpfile, "r");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3489
Status	New

The *syms__load_file method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-	iovisor@@bcc-0.29.0-CVE-2021-3520-

	FP.c	FP.c
Line	665	665
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
665.        f = fopen(fname, "r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3490
Status	New

The *partitions__load method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	842	842
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
842.        f = fopen("/proc/partitions", "r");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3491
Status	New

The is_kernel_module method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1011	1011
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1011.       f = fopen("/proc/modules", "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3492
Status	New

The kprobe_exists method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1113	1113
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1113.       f = fopen("/sys/kernel/debug/kprobes/blacklist", "r");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3493
Status	New

The kprobe_exists method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1133	1133
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1133.       f = fopen(tracefs_available_filter_functions(), "r");
```

TOCTOU\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3494
Status New

The kprobe_exists method in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1155	1155
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1155.       f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3495
Status New

The *ksyms__load method in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	104	104
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
104.        f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3496
Status New

The create_tmp_vdso_image method in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	540	540
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
540.        f = fopen(tmpfile, "r");
```

TOCTOU\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3497
Status New

The *syms__load_file method in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	651	651
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
651.        f = fopen(fname, "r");
```

TOCTOU\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3498
Status New

The *partitions__load method in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	809	809
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
809.        f = fopen("/proc/partitions", "r");
```

TOCTOU\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3499
Status New

The is_kernel_module method in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	986	986
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
986.        f = fopen("/proc/modules", "r");
```

TOCTOU\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3500
Status New

The kprobe_exists method in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1062	1062
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1062.       f =
fopen("/sys/kernel/debug/tracing/available_filter_functions", "r");
```

TOCTOU\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3501
Status New

The kprobe_exists method in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1084	1084
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1084.        f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3502
Status	New

The *ksyms__load method in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	104	104
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
104.        f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3503
Status	New

The create_tmp_vdso_image method in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	540	540
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
540.        f = fopen(tmpfile, "r");
```

TOCTOU\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3504
Status New

The *syms__load_file method in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	651	651
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
651.        f = fopen(fname, "r");
```

TOCTOU\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3505

Status	New

The *partitions__load method in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	809	809
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
809.        f = fopen("/proc/partitions", "r");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3506
Status	New

The is_kernel_module method in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	986	986
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
986.        f = fopen("/proc/modules", "r");
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=3507
Status	New

The kprobe_exists method in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	1062	1062
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1062.       f =
fopen("/sys/kernel/debug/tracing/available_filter_functions", "r");
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3508
Status	New

The kprobe_exists method in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	1084	1084
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1084.       f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3509
Status	New

The *ksyms__load method in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	105	105
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
105.        f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3510
Status	New

The create_tmp_vdso_image method in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	541	541
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
541.        f = fopen(tmpfile, "r");
```

TOCTOU\Path 25:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3511
Status	New

The *syms__load_file method in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	652	652
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
652.        f = fopen(fname, "r");
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3512
Status	New

The *partitions__load method in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	810	810
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
810.        f = fopen("/proc/partitions", "r");
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3513
Status	New

The is_kernel_module method in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	977	977
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
977.        f = fopen("/proc/modules", "r");
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3514
Status	New

The kprobe_exists method in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1067	1067
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1067.       f =
fopen("/sys/kernel/debug/tracing/available_filter_functions", "r");
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3515
Status	New

The kprobe_exists method in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1089	1089
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1089.       f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3516
Status	New

The *ksyms__load method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	106	106
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
106.        f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3517
Status	New

The create_tmp_vdso_image method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	551	551
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
551.        f = fopen(tmpfile, "r");
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3518
Status	New

The *syms__load_file method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	666	666
Object	fopen	fopen

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Method	struct syms *syms__load_file(const char *fname)

```
....
666.        f = fopen(fname, "r");
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3519
Status	New

The *partitions__load method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	843	843
Object	fopen	fopen

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	struct partitions *partitions__load(void)

```
....
843.        f = fopen("/proc/partitions", "r");
```

TOCTOU\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3520
Status	New

The is_kernel_module method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1012	1012
Object	fopen	fopen

Code Snippet

File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	bool is_kernel_module(const char *name)

```
....
1012.       f = fopen("/proc/modules", "r");
```

TOCTOU\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3521
Status	New

The kprobe_exists method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1114	1114
Object	fopen	fopen

Code Snippet

File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	bool kprobe_exists(const char *name)

```
....
1114.       f = fopen("/sys/kernel/debug/kprobes/blacklist", "r");
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3522
Status	New

The kprobe_exists method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1134	1134
Object	fopen	fopen

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	bool kprobe_exists(const char *name)

```
....
1134.       f = fopen(tracefs_available_filter_functions(), "r");
```

TOCTOU\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3523
Status	New

The kprobe_exists method in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1156	1156
Object	fopen	fopen

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	bool kprobe_exists(const char *name)

```
....
1156.       f = fopen("/proc/kallsyms", "r");
```

TOCTOU\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3524
Status	New

The dump_open method in irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Line	1383	1383
Object	fopen	fopen

Code Snippet	
File Name	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Method	dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1383.          FILE *fp = fopen(dumpfile,"wb+");
```

TOCTOU\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3525
Status	New

The dump_open method in irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Line	1383	1383
Object	fopen	fopen

Code Snippet	
File Name	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Method	dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1383.          FILE *fp = fopen(dumpfile,"wb+");
```

TOCTOU\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3526
Status	New

The dump_open method in irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Line	1383	1383

Object	fopen	fopen

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Method dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1383.           FILE *fp = fopen(dumpfile,"wb+");
```

TOCTOU\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3527
Status	New

The dump_open method in irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Line	1396	1396
Object	fopen	fopen

Code Snippet
File Name irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Method dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1396.           FILE *fp = fopen(dumpfile,"wb+");
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3528
Status	New

The setoutput method in jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c

Line	607	607
Object	fopen	fopen

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method void setoutput(char *filename)

```
....
607.      outfile = fopen(filename, Hflag? "wb":"wt");
```

TOCTOU\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3529
Status	New

The setoutput method in jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	607	607
Object	fopen	fopen

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method void setoutput(char *filename)

```
....
607.      outfile = fopen(filename, Hflag? "wb":"wt");
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3530
Status	New

The init_aliases method in jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-	jedisct1@@pure-ftpd-1.0.50-CVE-2020-

	9274-TP.c	9274-TP.c
Line	23	23
Object	fopen	fopen

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
23.      if ((fp = fopen(ALIASES_FILE, "r")) == NULL) {
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3531
Status	New

The init_aliases method in jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	23	23
Object	fopen	fopen

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
23.      if ((fp = fopen(ALIASES_FILE, "r")) == NULL) {
```

TOCTOU\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3532
Status	New

The main method in iovisor@@bcc-v0.26.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	iovisor@@bcc-v0.26.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.26.0-CVE-2021-3520-FP.c
Line	312	312
Object	open	open

Code Snippet
File Name iovisor@@bcc-v0.26.0-CVE-2021-3520-FP.c
Method int main(int argc, char **argv)

```
....
312.              cgfd = open(env.cgroupspath, O_RDONLY);
```

TOCTOU\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3533
Status New

The main method in iovisor@@bcc-v0.27.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.27.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.27.0-CVE-2021-3520-FP.c
Line	311	311
Object	open	open

Code Snippet
File Name iovisor@@bcc-v0.27.0-CVE-2021-3520-FP.c
Method int main(int argc, char **argv)

```
....
311.              cgfd = open(env.cgroupspath, O_RDONLY);
```

TOCTOU\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3534
Status New

The main method in iovisor@@bcc-v0.31.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	iovisor@@bcc-v0.31.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.31.0-CVE-2021-3520-FP.c
Line	346	346
Object	open	open

Code Snippet
File Name iovisor@@bcc-v0.31.0-CVE-2021-3520-FP.c
Method int main(int argc, char **argv)

```
....
346.              cgfd = open(env.cgroupspath, O_RDONLY);
```

TOCTOU\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3535
Status New

The Helper::flushPageCache method in JonMagon@@KDiskMark-3.0.0-CVE-2022-40673-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	JonMagon@@KDiskMark-3.0.0-CVE-2022-40673-TP.c	JonMagon@@KDiskMark-3.0.0-CVE-2022-40673-TP.c
Line	159	159
Object	open	open

Code Snippet
File Name JonMagon@@KDiskMark-3.0.0-CVE-2022-40673-TP.c
Method QVariantMap Helper::flushPageCache()

```
....
159.      if (file.open(QIODevice::WriteOnly | QIODevice::Text)) {
```

TOCTOU\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3536
Status New

The LibarchivePlugin::copyData method in KDE@@ark-v21.11.80-CVE-2020-24654-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Line	507	507
Object	open	open

Code Snippet
File Name KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Method void LibarchivePlugin::copyData(const QString& filename, struct archive *dest, bool partialprogress)

```
....
507.      if (!file.open(QIODevice::ReadOnly)) {
```

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=1020038&projectid=20031&pathid=3407
Status	New

	Source	Destination
File	koekeishiya@@yabai-v7.0.4-CVE-2021-3520-FP.c	koekeishiya@@yabai-v7.0.4-CVE-2021-3520-FP.c
Line	2834	2834
Object	chmod	chmod

Code Snippet
File Name koekeishiya@@yabai-v7.0.4-CVE-2021-3520-FP.c
Method bool message_loop_begin(char *socket_path)

```
....
2834.      if (chmod(socket_path, 0600) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3408
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	106	106
Object	f	f

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
106.        f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3409
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	551	551
Object	f	f

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
551.        f = fopen(tmpfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3410
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-	iovisor@@bcc-0.29.0-CVE-2021-3520-

	FP.c	FP.c
Line	665	665
Object	f	f

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
665.        f = fopen(fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3411
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	842	842
Object	f	f

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
842.        f = fopen("/proc/partitions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3412
Status New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1011	1011
Object	f	f

Code Snippet

File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	bool is_kernel_module(const char *name)

```
....
1011.       f = fopen("/proc/modules", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3413
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1113	1113
Object	f	f

Code Snippet

File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	bool kprobe_exists(const char *name)

```
....
1113.       f = fopen("/sys/kernel/debug/kprobes/blacklist", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3414
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1133	1133
Object	f	f

Code Snippet

File Name	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method	bool kprobe_exists(const char *name)

```
....
1133.       f = fopen(tracefs_available_filter_functions(), "r");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3415
Status	New

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1155	1155
Object	f	f

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1155.       f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3416
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	104	104
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
104.        f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3417
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	540	540
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
540.         f = fopen(tmpfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3418
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	651	651
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
651.         f = fopen(fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3419
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	809	809

Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
809.        f = fopen("/proc/partitions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3420
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	986	986
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
986.        f = fopen("/proc/modules", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3421
Status New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1062	1062
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1062.       f =
fopen("/sys/kernel/debug/tracing/available_filter_functions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3422
Status	New

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	1084	1084
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1084.       f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3423
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	104	104
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
104.        f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3424
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	540	540
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
540.         f = fopen(tmpfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3425
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	651	651
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
651.         f = fopen(fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3426
Status	New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	809	809
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
809.        f = fopen("/proc/partitions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3427
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	986	986
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
986.        f = fopen("/proc/modules", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3428
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	1062	1062

Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1062.       f =
fopen("/sys/kernel/debug/tracing/available_filter_functions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3429
Status New

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	1084	1084
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1084.       f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3430
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	105	105
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
105.        f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3431
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	541	541
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
541.        f = fopen(tmpfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3432
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	652	652
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
652.        f = fopen(fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3433
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	810	810
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
810.        f = fopen("/proc/partitions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3434
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	977	977
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
977.        f = fopen("/proc/modules", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3435
Status	New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1067	1067
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1067.       f =
fopen("/sys/kernel/debug/tracing/available_filter_functions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3436
Status New

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1089	1089
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1089.       f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3437
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	106	106

Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct ksyms *ksyms__load(void)

```
....
106.        f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3438
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	551	551
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
551.        f = fopen(tmpfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3439
Status New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	666	666
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct syms *syms__load_file(const char *fname)

```
....
666.        f = fopen(fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3440
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	843	843
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
843.        f = fopen("/proc/partitions", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3441
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1012	1012
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1012.       f = fopen("/proc/modules", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3442
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1114	1114
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1114.       f = fopen("/sys/kernel/debug/kprobes/blacklist", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3443
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1134	1134
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1134.       f = fopen(tracefs_available_filter_functions(), "r");
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3444
Status	New

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	1156	1156
Object	f	f

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool kprobe_exists(const char *name)

```
....
1156.       f = fopen("/proc/kallsyms", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3445
Status New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	607	607
Object	outfile	outfile

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method void setoutput(char *filename)

```
....
607.      outfile = fopen(filename, Hflag? "wb":"wt");
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3446
Status New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	607	607

Object	outfile	outfile

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method void setoutput(char *filename)

```
....
607.      outfile = fopen(filename, Hflag? "wb":"wt");
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3447
Status New

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	23	23
Object	fp	fp

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
23.      if ((fp = fopen(ALIASES_FILE, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3448
Status New

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	23	23
Object	fp	fp

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
23.      if ((fp = fopen(ALIASES_FILE, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3449
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Line	1383	1383
Object	fp	fp

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-31981-TP.c
Method dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1383.          FILE *fp = fopen(dumpfile,"wb+");
```

Incorrect Permission Assignment For Critical Resources\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3450
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Line	1383	1383
Object	fp	fp

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-31982-TP.c
Method dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1383.          FILE *fp = fopen(dumpfile,"wb+");
```

Incorrect Permission Assignment For Critical Resources\Path 45:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3451
Status	New

	Source	Destination
File	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Line	1383	1383
Object	fp	fp

Code Snippet
File Name irontec@@sngrep-v1.6.0-CVE-2023-36192-TP.c
Method dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1383.           FILE *fp = fopen(dumpfile,"wb+");
```

Incorrect Permission Assignment For Critical Resources\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3452
Status	New

	Source	Destination
File	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c	irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Line	1396	1396
Object	fp	fp

Code Snippet
File Name irontec@@sngrep-v1.7.0-CVE-2023-36192-TP.c
Method dump_open(const char *dumpfile, ino_t* dump_inode)

```
....
1396.           FILE *fp = fopen(dumpfile,"wb+");
```

Incorrect Permission Assignment For Critical Resources\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3453
Status	New

	Source	Destination
File	JonMagon@@KDiskMark-3.0.0-CVE-2022-40673-TP.c	JonMagon@@KDiskMark-3.0.0-CVE-2022-40673-TP.c
Line	159	159
Object	open	open

Code Snippet
File Name JonMagon@@KDiskMark-3.0.0-CVE-2022-40673-TP.c
Method QVariantMap Helper::flushPageCache()

```
....
159.      if (file.open(QIODevice::WriteOnly | QIODevice::Text)) {
```

Incorrect Permission Assignment For Critical Resources\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3454
Status New

	Source	Destination
File	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c	KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Line	507	507
Object	open	open

Code Snippet
File Name KDE@@ark-v21.11.80-CVE-2020-24654-TP.c
Method void LibarchivePlugin::copyData(const QString& filename, struct archive *dest, bool partialprogress)

```
....
507.      if (!file.open(QIODevice::ReadOnly)) {
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2053
Status New

	Source	Destination

File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	265	265
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
265.          if (pattern >= maxpattern-1) patterns = xrealloc(patterns,
sizeof(char *) * (maxpattern += 10));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2054
Status New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	274	274
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
274.          if (ipattern >= maxipattern-1) ipatterns =
xrealloc(ipatterns, sizeof(char *) * (maxipattern += 10));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2055
Status New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	541	541

Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
541.        if (!dirname) dirname = (char **)xmalloc(sizeof(char *) *
(q=MINIT));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2056
Status New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	542	542
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
542.        else if (p == (q-2)) dirname = (char
**)xrealloc(dirname,sizeof(char *) * (q+=MINC));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2057
Status New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	560	560
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c

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

```
....
560.      dirname = xmalloc(sizeof(char *) * 2);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2058
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	844	844
Object	sizeof	sizeof

Code Snippet	
File Name	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method	struct _info **read_dir(char *dir, int *n, int infotop)

```
....
844.    dl = (struct _info **)xmalloc(sizeof(struct _info *) * (ne =
MINIT));
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2059
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	859	859
Object	sizeof	sizeof

Code Snippet	
File Name	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method	struct _info **read_dir(char *dir, int *n, int infotop)

```
....
859.        info->comment = xmalloc(sizeof(char *) * (i+1));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2060
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	863	863
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
863.         if (p == (ne-1)) dl = (struct _info
**)xrealloc(dl,sizeof(struct _info *) * (ne += MINC));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2061
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	1003	1003
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
1003.     if (topsort) qsort(sav,n,sizeof(struct _info *),topsort);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2062
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	265	265
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
265.          if (pattern >= maxpattern-1) patterns = xrealloc(patterns,
sizeof(char *) * (maxpattern += 10));
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2063
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	274	274
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
274.          if (ipattern >= maxipattern-1) ipatterns =
xrealloc(ipatterns, sizeof(char *) * (maxipattern += 10));
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2064
Status	New

	Source	Destination

File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	541	541
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
541.        if (!dirname) dirname = (char **)xmalloc(sizeof(char *) *
(q=MINIT));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2065
Status New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	542	542
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
542.        else if (p == (q-2)) dirname = (char
**)xrealloc(dirname,sizeof(char *) * (q+=MINC));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2066
Status New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	560	560

Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

```
....
560.      dirname = xmalloc(sizeof(char *) * 2);
```

Use of Sizeof On a Pointer Type\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2067
Status New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	844	844
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
844.    dl = (struct _info **)xmalloc(sizeof(struct _info *) * (ne =
MINIT));
```

Use of Sizeof On a Pointer Type\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2068
Status New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	859	859
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
859.        info->comment = xmalloc(sizeof(char *) * (i+1));
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2069
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	863	863
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
863.        if (p == (ne-1)) dl = (struct _info
**)xrealloc(dl,sizeof(struct _info *) * (ne += MINC));
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2070
Status	New

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	1003	1003
Object	sizeof	sizeof

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
1003.    if (topsort) qsort(sav,n,sizeof(struct _info *),topsort);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2071
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	47	47
Object	sizeof	sizeof

Code Snippet

File Name koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c

Method static struct window **window_manager_find_windows_for_spaces(uint64_t *space_list, int space_count, int *window_aggregate_count)

```
....
47.      struct window **window_aggregate_list =
ts_alloc_aligned(sizeof(struct window *), window_count);
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2072
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	951	951
Object	sizeof	sizeof

Code Snippet

File Name koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c

Method struct window **window_manager_find_application_windows(struct window_manager *wm, struct application *application, int *window_count)

```
....
951.      struct window **window_list = ts_alloc_aligned(sizeof(struct
window *), wm->window.count);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2073
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	32	32
Object	sizeof	sizeof

Code Snippet

File Name koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c

Method static struct window **window_manager_find_windows_for_spaces(uint64_t *space_list, int space_count, int *window_aggregate_count)

```
....
32.      struct window **window_aggregate_list =
ts_alloc_aligned(sizeof(struct window *), window_count);
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2074
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	950	950
Object	sizeof	sizeof

Code Snippet

File Name koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c

Method struct window **window_manager_find_application_windows(struct window_manager *wm, struct application *application, int *window_count)

```
....
950.      struct window **window_list = ts_alloc_aligned(sizeof(struct
window *), wm->window.count);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2075

Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	32	32
Object	sizeof	sizeof

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method static struct window **window_manager_find_windows_for_spaces(uint64_t *space_list, int space_count, int *window_aggregate_count)

```
....
32.      struct window **window_aggregate_list =
ts_alloc_aligned(sizeof(struct window *), window_count);
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2076
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1387	1387
Object	sizeof	sizeof

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method struct window **window_manager_find_application_windows(struct window_manager *wm, struct application *application, int *window_count)

```
....
1387.      struct window **window_list = ts_alloc_aligned(sizeof(struct
window *), wm->window.count);
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2077
Status	New

	Source	Destination

File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1479	1479
Object	sizeof	sizeof

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method struct window **window_manager_add_application_windows(struct space_manager *sm, struct window_manager *wm, struct application *application, int *count)

```
....
1479.      struct window **list = ts_alloc_aligned(sizeof(struct window
*), window_count);
```

Use of Sizeof On a Pointer Type\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2078
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Line	779	779
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2022-42898-TP.c
Method mspac_export_authdata(krb5_context kcontext,

```
....
779.      authdata = calloc(2, sizeof(krb5_authdata *));
```

Use of Sizeof On a Pointer Type\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2079
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Line	666	666

Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
666.                    sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2080
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Line	963	963
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2023-36054-TP.c
Method xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
963.                    sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2081
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	887	887
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
887.              t = realloc(db_args, sizeof(char *) * (db_args_size +
1));  /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2082
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Line	779	779
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2022-42898-TP.c
Method mspac_export_authdata(krb5_context kcontext,

```
....
779.      authdata = calloc(2, sizeof(krb5_authdata *));
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2083
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Line	666	666
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
666.                      sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2084
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Line	963	963
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2023-36054-TP.c
Method xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
963.                    sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2085
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	887	887
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
887.              t = realloc(db_args, sizeof(char *) * (db_args_size +
1));  /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2086
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Line	779	779
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2022-42898-TP.c
Method mspac_export_authdata(krb5_context kcontext,

```
....
779.      authdata = calloc(2, sizeof(krb5_authdata *));
```

Use of Sizeof On a Pointer Type\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2087
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Line	666	666
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
666.                      sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2088
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Line	963	963

Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2023-36054-FP.c
Method xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
963.                        sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2089
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	887	887
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
887.              t = realloc(db_args, sizeof(char *) * (db_args_size +
1));  /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2090
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Line	779	779
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2022-42898-TP.c
Method mspac_export_authdata(krb5_context kcontext,

```
....
779.      authdata = calloc(2, sizeof(krb5_authdata *));
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2091
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c
Line	666	666
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
666.                      sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2092
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c
Line	963	963
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2023-36054-TP.c
Method xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
963.                      sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2093
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	887	887
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
887.              t = realloc(db_args, sizeof(char *) * (db_args_size +
1));  /* 1 for NULL */
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2094
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Line	779	779
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2022-42898-TP.c
Method mspac_export_authdata(krb5_context kcontext,

```
....
779.      authdata = calloc(2, sizeof(krb5_authdata *));
```

Use of Sizeof On a Pointer Type\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2095
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c
Line	666	666
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c
Method xdr_gprincs_ret(XDR *xdrs, gprincs_ret *objp)

```
....
666.                    sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2096
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c
Line	963	963
Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2023-36054-TP.c
Method xdr_gpols_ret(XDR *xdrs, gpols_ret *objp)

```
....
963.                    sizeof(char *), xdr_nullstring)) {
```

Use of Sizeof On a Pointer Type\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2097
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Line	887	887

Object	sizeof	sizeof

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
887.              t = realloc(db_args, sizeof(char *) * (db_args_size +
1));  /* 1 for NULL */
```

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=1020038&projectid=20031&pathid=3455
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	584	592
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
584.                    strerror(errno));
....
592.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

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=1020038&projectid=20

	031&pathid=3456
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	590	592
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
590.                    strerror(errno));
....
592.             fprintf(stderr, "failed to write to vDSO image: %s\n",
```

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=1020038&projectid=20031&pathid=3457
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	593	592
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
593.                    strerror(errno));
....
592.             fprintf(stderr, "failed to write to vDSO image: %s\n",
```

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=1020038&projectid=20031&pathid=3458
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	584	589
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
584.                    strerror(errno));
....
589.              fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

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=1020038&projectid=20031&pathid=3459
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	590	589
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
590.                    strerror(errno));
....
589.                fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

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=1020038&projectid=20031&pathid=3460
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	584	583
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
584.                    strerror(errno));
....
583.                fprintf(stderr, "failed to create temp file: %s\n",
```

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=1020038&projectid=20031&pathid=3461
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	572	580
Object	errno	fprintf

Code Snippet	
File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
572.                    strerror(errno));
....
580.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3462
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	578	580
Object	errno	fprintf

Code Snippet	
File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
578.                    strerror(errno));
....
580.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3463
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-	iovisor@@bcc-v0.21.0-CVE-2021-3520-

	FP.c	FP.c
Line	581	580
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
581.                    strerror(errno));
....
580.             fprintf(stderr, "failed to write to vDSO image: %s\n",
```

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=1020038&projectid=20031&pathid=3464
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	572	577
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
572.                    strerror(errno));
....
577.             fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

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=1020038&projectid=20031&pathid=3465
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	578	577
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
578.                    strerror(errno));
....
577.              fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

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=1020038&projectid=20031&pathid=3466
Status New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	572	571
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
572.                    strerror(errno));
....
571.              fprintf(stderr, "failed to create temp file: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3467
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	572	580
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
572.                    strerror(errno));
....
580.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3468
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	578	580
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
578.                    strerror(errno));
....
580.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3469
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	581	580
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
581.                    strerror(errno));
....
580.             fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3470
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	572	577
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
572.                    strerror(errno));
....
577.                fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3471
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	578	577
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
578.                    strerror(errno));
....
577.                fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3472
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 527.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	572	571
Object	errno	fprintf

Code Snippet	
File Name	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
572.                    strerror(errno));
....
571.              fprintf(stderr, "failed to create temp file: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3473
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	573	581
Object	errno	fprintf

Code Snippet	
File Name	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
573.                    strerror(errno));
....
581.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3474
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-	iovisor@@bcc-v0.25.0-CVE-2021-3520-

	FP.c	FP.c
Line	579	581
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
579.                    strerror(errno));
....
581.             fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3475
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	582	581
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
582.                    strerror(errno));
....
581.             fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3476
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	573	578
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
573.                    strerror(errno));
....
578.              fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

Exposure of System Data to Unauthorized Control Sphere\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3477
Status New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	579	578
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
579.                    strerror(errno));
....
578.              fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

Exposure of System Data to Unauthorized Control Sphere\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3478
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 528.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	573	572
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
573.                    strerror(errno));
....
572.                fprintf(stderr, "failed to create temp file: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3479
Status	New

The system data read by fentry_can_attach in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 1024 is potentially exposed by fentry_can_attach found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 1024.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1033	1034
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool fentry_can_attach(const char *name, const char *mod)

```
....
1033.               err = -errno;
1034.               fprintf(stderr, "failed to parse vmlinux BTF at '%s':
%s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3480
Status	New

The system data read by fentry_can_attach in the file iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 1024 is potentially exposed by fentry_can_attach found in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 1024.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	1042	1043
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method bool fentry_can_attach(const char *name, const char *mod)

```
....
1042.                   err = -errno;
1043.                   fprintf(stderr, "failed to load BTF from %s:
%s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3481
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	584	592
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
584.                    strerror(errno));
....
592.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3482
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	590	592
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
590.                    strerror(errno));
....
592.              fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3483
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	593	592
Object	errno	fprintf

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
593.                    strerror(errno));
....
592.             fprintf(stderr, "failed to write to vDSO image: %s\n",
```

Exposure of System Data to Unauthorized Control Sphere\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3484
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	584	589
Object	errno	fprintf

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
584.                    strerror(errno));
....
589.             fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

Exposure of System Data to Unauthorized Control Sphere\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3485
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-	iovisor@@bcc-v0.30.0-CVE-2021-3520-

	FP.c	FP.c
Line	590	589
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
590.                    strerror(errno));
....
589.             fprintf(stderr, "failed to unlink %s: %s\n", tmpfile,
```

Exposure of System Data to Unauthorized Control Sphere\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3486
Status	New

The system data read by create_tmp_vdso_image in the file iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538 is potentially exposed by create_tmp_vdso_image found in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 538.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	584	583
Object	errno	fprintf

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
584.                    strerror(errno));
....
583.             fprintf(stderr, "failed to create temp file: %s\n",
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2446
Status	New

The size of the buffer used by *partitions__load in "%u %u %llu %s", at line 833 of iovisor@@bcc-0.29.0-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 *partitions__load passes to "%u %u %llu %s", at line 833 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	854	854
Object	"%u %u %llu %s"	"%u %u %llu %s"

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
854.                if (sscanf(buf, "%u %u %llu %s", &devmaj, &devmin,
&nop,
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2447
Status	New

The size of the buffer used by is_kernel_module in "%s %*s\n", at line 1005 of iovisor@@bcc-0.29.0-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 is_kernel_module passes to "%s %*s\n", at line 1005 of iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	1016	1016
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1016.               if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2448
Status	New

The size of the buffer used by *partitions__load in "%u %u %llu %s", at line 800 of iovisor@@bcc-v0.21.0-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 *partitions__load passes to "%u %u %llu %s", at line 800 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	821	821
Object	"%u %u %llu %s"	"%u %u %llu %s"

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
821.                if (sscanf(buf, "%u %u %llu %s", &devmaj, &devmin,
&nop,
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2449
Status	New

The size of the buffer used by is_kernel_module in "%s %*s\n", at line 980 of iovisor@@bcc-v0.21.0-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 is_kernel_module passes to "%s %*s\n", at line 980 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	991	991
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
991.              if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2450
Status	New

The size of the buffer used by *partitions__load in "%u %u %llu %s", at line 800 of iovisor@@bcc-v0.23.0-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 *partitions__load passes to "%u %u %llu %s", at line 800 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	821	821
Object	"%u %u %llu %s"	"%u %u %llu %s"

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method struct partitions *partitions__load(void)

```
....
821.              if (sscanf(buf, "%u %u %llu %s", &devmaj, &devmin,
&nop,
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2451
Status	New

The size of the buffer used by is_kernel_module in "%s %*s\n", at line 980 of iovisor@@bcc-v0.23.0-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 is_kernel_module passes to "%s %*s\n", at line 980 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	991	991
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet

File Name	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method	bool is_kernel_module(const char *name)

```
....
991.              if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2452
Status	New

The size of the buffer used by *partitions__load in "%u %u %llu %s", at line 801 of iovisor@@bcc-v0.25.0-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 *partitions__load passes to "%u %u %llu %s", at line 801 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	822	822
Object	"%u %u %llu %s"	"%u %u %llu %s"

Code Snippet

File Name	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method	struct partitions *partitions__load(void)

```
....
822.              if (sscanf(buf, "%u %u %llu %s", &devmaj, &devmin,
&nop,
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2453
Status	New

The size of the buffer used by is_kernel_module in "%s %*s\n", at line 971 of iovisor@@bcc-v0.25.0-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 is_kernel_module passes to "%s %*s\n", at line 971 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	982	982
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet	
File Name	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method	bool is_kernel_module(const char *name)

```
....
982.              if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2454
Status	New

The size of the buffer used by *partitions__load in "%u %u %llu %s", at line 834 of iovisor@@bcc-v0.30.0-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 *partitions__load passes to "%u %u %llu %s", at line 834 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	855	855
Object	"%u %u %llu %s"	"%u %u %llu %s"

Code Snippet	
File Name	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method	struct partitions *partitions__load(void)

```
....
855.              if (sscanf(buf, "%u %u %llu %s", &devmaj, &devmin,
&nop,
```

Potential Precision Problem\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2455
Status	New

The size of the buffer used by is_kernel_module in "%s %*s\n", at line 1006 of iovisor@@bcc-v0.30.0-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 is_kernel_module passes to "%s %*s\n", at line 1006 of iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c

Line	1017	1017
Object	"%s %*s\n"	"%s %*s\n"

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method bool is_kernel_module(const char *name)

```
....
1017.             if (sscanf(buf, "%s %*s\n", buf) != 1)
```

Potential Precision Problem\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2456
Status	New

The size of the buffer used by *fillinfo in " %s", at line 1438 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *fillinfo passes to " %s", at line 1438 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	1449	1449
Object	" %s"	" %s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method char *fillinfo(char *buf, struct _info *ent)

```
....
1449.    if (pflag) n += sprintf(buf+n, " %s",prot(ent->attr));
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2457
Status	New

The size of the buffer used by *fillinfo in " %s", at line 1438 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *fillinfo passes to " %s", at line 1438 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-	jart@@cosmopolitan-3.3.1-CVE-2024-

	6381-TP.c	6381-TP.c
Line	1456	1456
Object	" %s"	" %s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method char *fillinfo(char *buf, struct _info *ent)

```
....
1456.    if (Dflag) n += sprintf(buf+n, " %s", do_date(cflag? ent->ctime
: ent->mtime));
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2458
Status	New

The size of the buffer used by print_version in "%.*s%s", at line 589 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_version passes to "%.*s%s", at line 589 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	593	593
Object	"%.*s%s"	"%.*s%s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method void print_version(int nl)

```
....
593.    sprintf(buf, "%.*s%s", (int)strlen(v)-2, v, nl?"\n":"");
```

Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2459
Status	New

The size of the buffer used by **read_dir in "%s%s", at line 826 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **read_dir passes to "%s%s", at line 826 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	852	852
Object	"%s%s"	"%s%s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
852.      if (es) sprintf(path, "%s%s", dir, ent->d_name);
```

Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2460
Status	New

The size of the buffer used by **read_dir in "%s/%s", at line 826 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **read_dir passes to "%s/%s", at line 826 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	853	853
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
853.      else sprintf(path,"%s/%s",dir,ent->d_name);
```

Potential Precision Problem\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2461
Status	New

The size of the buffer used by **unix_getfulltree in "%s%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that **unix_getfulltree passes to "%s%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	973	973
Object	"%s%s"	"%s%s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
973.              if (fflag && !strcmp(d,"/"))
sprintf(path,"%s%s",d,(*dir)->lnk);
```

Potential Precision Problem\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2462
Status New

The size of the buffer used by **unix_getfulltree in "%s/%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **unix_getfulltree passes to "%s/%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	974	974
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
974.              else sprintf(path,"%s/%s",d,(*dir)->lnk);
```

Potential Precision Problem\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2463

Status	New

The size of the buffer used by **unix_getfulltree in "%s%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **unix_getfulltree passes to "%s%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	981	981
Object	"%s%s"	"%s%s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
981.        if (fflag && !strcmp(d,"/")) sprintf(path,"%s%s",d,(*dir)->name);
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2464
Status	New

The size of the buffer used by **unix_getfulltree in "%s/%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **unix_getfulltree passes to "%s/%s", at line 894 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	982	982
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
982.        else sprintf(path,"%s/%s",d,(*dir)->name);
```

Potential Precision Problem\Path 20:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2465
Status	New

The size of the buffer used by *fillinfo in " %s", at line 1438 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *fillinfo passes to " %s", at line 1438 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	1449	1449
Object	" %s"	" %s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method char *fillinfo(char *buf, struct _info *ent)

```
....
1449.    if (pflag) n += sprintf(buf+n, " %s",prot(ent->attr));
```

Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2466
Status	New

The size of the buffer used by *fillinfo in " %s", at line 1438 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *fillinfo passes to " %s", at line 1438 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	1456	1456
Object	" %s"	" %s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method char *fillinfo(char *buf, struct _info *ent)

```
....
1456.    if (Dflag) n += sprintf(buf+n, " %s", do_date(cflag? ent->ctime
: ent->mtime));
```

Potential Precision Problem\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2467
Status	New

The size of the buffer used by print_version in "%.*s%s", at line 589 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_version passes to "%.*s%s", at line 589 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	593	593
Object	"%.*s%s"	"%.*s%s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method void print_version(int nl)

```
....
593.    sprintf(buf, "%.*s%s", (int)strlen(v)-2, v, nl?"\n":"");
```

Potential Precision Problem\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2468
Status	New

The size of the buffer used by **read_dir in "%s%s", at line 826 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **read_dir passes to "%s%s", at line 826 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	852	852
Object	"%s%s"	"%s%s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
852.      if (es) sprintf(path, "%s%s", dir, ent->d_name);
```

Potential Precision Problem\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2469
Status	New

The size of the buffer used by **read_dir in "%s/%s", at line 826 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **read_dir passes to "%s/%s", at line 826 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	853	853
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **read_dir(char *dir, int *n, int infotop)

```
....
853.      else sprintf(path,"%s/%s",dir,ent->d_name);
```

Potential Precision Problem\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2470
Status	New

The size of the buffer used by **unix_getfulltree in "%s%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **unix_getfulltree passes to "%s%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	973	973
Object	"%s%s"	"%s%s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
973.                if (fflag && !strcmp(d,"/"))
sprintf(path,"%s%s",d,(*dir)->lnk);
```

Potential Precision Problem\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2471
Status	New

The size of the buffer used by **unix_getfulltree in "%s/%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **unix_getfulltree passes to "%s/%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	974	974
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
974.                else sprintf(path,"%s/%s",d,(*dir)->lnk);
```

Potential Precision Problem\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2472
Status	New

The size of the buffer used by **unix_getfulltree in "%s%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **unix_getfulltree passes to "%s%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	981	981
Object	"%s%s"	"%s%s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
981.        if (fflag && !strcmp(d,"/")) sprintf(path,"%s%s",d,(*dir)->name);
```

Potential Precision Problem\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2473
Status New

The size of the buffer used by **unix_getfulltree in "%s/%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **unix_getfulltree passes to "%s/%s", at line 894 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c, to overwrite the target buffer.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	982	982
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method struct _info **unix_getfulltree(char *d, u_long lev, dev_t dev, off_t *size, char **err)

```
....
982.        else sprintf(path,"%s/%s",d,(*dir)->name);
```

Heuristic 2nd Order Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow malloc Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow malloc\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2423

Status	New

The size of the buffer used by init_aliases in Pointer, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to alias, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	26	59
Object	alias	Pointer

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.      while (fgets(alias, sizeof alias, fp) != NULL) {
....
59.              if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2424
Status	New

The size of the buffer used by init_aliases in Pointer, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to dir, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	39	59
Object	dir	Pointer

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.              if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
....
59.              if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2425
Status	New

The size of the buffer used by init_aliases in curr, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to alias, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	26	59
Object	alias	curr

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.      while (fgets(alias, sizeof alias, fp) != NULL) {
....
59.              if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2426
Status	New

The size of the buffer used by init_aliases in curr, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to dir, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	39	59
Object	dir	curr

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.             if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2427
Status	New

The size of the buffer used by init_aliases in sizeof, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to alias, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	26	59
Object	alias	sizeof

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.      while (fgets(alias, sizeof alias, fp) != NULL) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2428
Status	New

The size of the buffer used by init_aliases in sizeof, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to dir, at line 17 of jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Line	39	59
Object	dir	sizeof

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.50-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.             if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2429
Status	New

The size of the buffer used by init_aliases in Pointer, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to alias, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	26	59
Object	alias	Pointer

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.     while (fgets(alias, sizeof alias, fp) != NULL) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2430
Status	New

The size of the buffer used by init_aliases in Pointer, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to dir, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-	jedisct1@@pure-ftpd-1.0.51-CVE-2020-

	9274-TP.c	9274-TP.c
Line	39	59
Object	dir	Pointer

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.             if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2431
Status	New

The size of the buffer used by init_aliases in curr, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to alias, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	26	59
Object	alias	curr

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.       while (fgets(alias, sizeof alias, fp) != NULL) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2432
Status	New

The size of the buffer used by init_aliases in curr, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that init_aliases passes to dir, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	39	59
Object	dir	curr

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.             if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2433
Status New

The size of the buffer used by init_aliases in sizeof, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to alias, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	26	59
Object	alias	sizeof

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
26.     while (fgets(alias, sizeof alias, fp) != NULL) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2434
Status	New

The size of the buffer used by init_aliases in sizeof, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_aliases passes to dir, at line 17 of jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c, to overwrite the target buffer.

	Source	Destination
File	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c	jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Line	39	59
Object	dir	sizeof

Code Snippet
File Name jedisct1@@pure-ftpd-1.0.51-CVE-2020-9274-TP.c
Method int init_aliases(void)

```
....
39.             if (fgets(dir, sizeof dir, fp) == NULL || *dir == 0) {
....
59.             if ((curr = malloc(sizeof *curr)) == NULL ||
```

Heuristic 2nd Order Buffer Overflow malloc\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2435
Status	New

The size of the buffer used by stszin in frame, at line 335 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that datain passes to data, at line 81 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	83	347
Object	data	frame

Code Snippet
File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int datain(void *data, int size)

```
....
83.      if (fread(data, 1, size, g_fin) != size)
```

File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c

Method	static int stszin(int size)

```
....
347.      mp4config.frame.data = malloc(sizeof(*mp4config.frame.data)
```

Heuristic 2nd Order Buffer Overflow malloc\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2436
Status	New

The size of the buffer used by stszin in ents, at line 335 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that datain passes to data, at line 81 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	83	348
Object	data	ents

Code Snippet

File Name	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method	static int datain(void *data, int size)

```
....
83.      if (fread(data, 1, size, g_fin) != size)
```

File Name	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method	static int stszin(int size)

```
....
348.                                    * (mp4config.frame.ents + 1));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2437
Status	New

The size of the buffer used by stszin in BinaryExpr, at line 335 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that datain passes to data, at line 81 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	83	348
Object	data	BinaryExpr

Code Snippet
File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int datain(void *data, int size)

```
....
83.      if (fread(data, 1, size, g_fin) != size)
```

File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int stszin(int size)

```
....
348.                                    * (mp4config.frame.ents + 1));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2438
Status	New

The size of the buffer used by stszin in BinaryExpr, at line 335 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that datain passes to data, at line 81 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	83	348
Object	data	BinaryExpr

Code Snippet
File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method static int datain(void *data, int size)

```
....
83.      if (fread(data, 1, size, g_fin) != size)
```

File Name knik0@@faad2-2_9_2-CVE-2021-32272-TP.c

Method	static int stszin(int size)

```
....
348.                                    * (mp4config.frame.ents + 1));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2439
Status	New

The size of the buffer used by stszin in frame, at line 335 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that datain passes to data, at line 81 of knik0@@faad2-2_9_2-CVE-2021-32272-TP.c, to overwrite the target buffer.

	Source	Destination
File	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Line	83	348
Object	data	frame

Code Snippet

File Name	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method	static int datain(void *data, int size)

```
....
83.      if (fread(data, 1, size, g_fin) != size)
```

File Name	knik0@@faad2-2_9_2-CVE-2021-32272-TP.c
Method	static int stszin(int size)

```
....
348.                                    * (mp4config.frame.ents + 1));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2440
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.21.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	546	562
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
562.        image = malloc(sz);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2441
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.21.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	546	562
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
562.        image = malloc(sz);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2442
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.23.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	546	562
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
562.        image = malloc(sz);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2443
Status New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.23.0-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 create_tmp_vdso_image passes to Address, at line 527 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	546	562
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.                            &start_addr, &end_addr, buf);
....
562.        image = malloc(sz);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 22:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2444
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 528 of iovisor@@bcc-v0.25.0-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 create_tmp_vdso_image passes to Address, at line 528 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	547	563
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
547.                            &start_addr, &end_addr, buf);
....
563.         image = malloc(sz);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2445
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 528 of iovisor@@bcc-v0.25.0-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 create_tmp_vdso_image passes to Address, at line 528 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	547	563
Object	Address	sz

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
547.                            &start_addr, &end_addr, buf);
....
563.        image = malloc(sz);
```

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=1020038&projectid=20031&pathid=3537
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	531	531
Object	relation_count	relation_count

Code Snippet
File Name koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Method bool window_manager_set_window_layer(struct window *window, int layer)

```
....
531.          parent_list[relation_count] =
SLSWindowIteratorGetParentID(iterator);
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3538
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Line	532	532
Object	relation_count	relation_count

Code Snippet	
File Name	koekeishiya@@yabai-v4.0.0-CVE-2021-3520-FP.c
Method	bool window_manager_set_window_layer(struct window *window, int layer)

```
....
532.            child_list[relation_count] =
SLSWindowIteratorGetWindowID(iterator);
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3539
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	515	515
Object	relation_count	relation_count

Code Snippet	
File Name	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Method	bool window_manager_set_window_layer(struct window *window, int layer)

```
....
515.            parent_list[relation_count] =
SLSWindowIteratorGetParentID(iterator);
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3540
Status	New

	Source	Destination
File	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Line	516	516
Object	relation_count	relation_count

Code Snippet	
File Name	koekeishiya@@yabai-v4.0.2-CVE-2021-3520-FP.c
Method	bool window_manager_set_window_layer(struct window *window, int layer)

```
....
516.          child_list[relation_count] =
SLSWindowIteratorGetWindowID(iterator);
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3541
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	806	806
Object	relation_count	relation_count

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method bool window_manager_set_window_layer(struct window *window, int layer)

```
....
806.          parent_list[relation_count] =
SLSWindowIteratorGetParentID(iterator);
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3542
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	807	807
Object	relation_count	relation_count

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method bool window_manager_set_window_layer(struct window *window, int layer)

```
....
807.          child_list[relation_count] =
SLSWindowIteratorGetWindowID(iterator);
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3543
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1825	1825
Object	a_list_index	a_list_index

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method enum window_op_error window_manager_swap_window(struct space_manager *sm, struct window_manager *wm, struct window *a, struct window *b)

```
....
1825.           a_node->window_list[a_list_index] = b->id;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3544
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1826	1826
Object	a_order_index	a_order_index

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method enum window_op_error window_manager_swap_window(struct space_manager *sm, struct window_manager *wm, struct window *a, struct window *b)

```
....
1826.           a_node->window_order[a_order_index] = b->id;
```

Unchecked Array Index\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3545
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1828	1828
Object	b_list_index	b_list_index

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method enum window_op_error window_manager_swap_window(struct space_manager *sm, struct window_manager *wm, struct window *a, struct window *b)

```
....
1828.           a_node->window_list[b_list_index] = a->id;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3546
Status	New

	Source	Destination
File	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c	koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Line	1829	1829
Object	b_order_index	b_order_index

Code Snippet
File Name koekeishiya@@yabai-v5.0.7-CVE-2021-3520-FP.c
Method enum window_op_error window_manager_swap_window(struct space_manager *sm, struct window_manager *wm, struct window *a, struct window *b)

```
....
1829.           a_node->window_order[b_order_index] = a->id;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3547
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Line	1553	1553
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1553.       bytes[buf.count] = 0;
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3548
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Line	895	895
Object	db_args_size	db_args_size

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
895.                db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3549
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Line	1555	1555

Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1555.       bytes[buf.count] = 0;
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3550
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Line	895	895
Object	db_args_size	db_args_size

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
895.              db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3551
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Line	1555	1555
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1555.       bytes[buf.count] = 0;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3552
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Line	895	895
Object	db_args_size	db_args_size

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
895.              db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3553
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Line	1543	1543
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1543.       bytes[buf.count] = 0;
```

Unchecked Array Index\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3554
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Line	895	895
Object	db_args_size	db_args_size

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
895.              db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3555
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Line	1543	1543
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1543.      bytes[buf.count] = 0;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3556
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Line	895	895
Object	db_args_size	db_args_size

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2024-6381-TP.c
Method extract_db_args_from_tl_data(krb5_context kcontext, krb5_tl_data **start,

```
....
895.              db_args[db_args_size] = NULL;
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=3557
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Line	1543	1543
Object	count	count

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Method k5_asn1_full_encode(const void *rep, const struct atype_info *a,

```
....
1543.      bytes[buf.count] = 0;
```

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=1020038&projectid=20031&pathid=2477

Status	New

	Source	Destination
File	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	402	402
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2478
Status	New

	Source	Destination
File	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	484	484
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2479
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c

Line	195	195
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Method k5_asn1_decode_int(const uint8_t *asn1, size_t len, intmax_t *val)

```
....
195.      if (len > sizeof(intmax_t) + (asn1[0] == 0))
```

Arithmenic Operation On Boolean\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2480
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c	krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.1-final-CVE-2020-28196-TP.c
Method k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2481
Status New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Line	195	195
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c

Method	k5_asn1_decode_int(const uint8_t *asn1, size_t len, intmax_t *val)

```
....
195.      if (len > sizeof(intmax_t) + (asn1[0] == 0))
```

Arithmenic Operation On Boolean\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2482
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.3-final-CVE-2020-28196-FP.c
Method k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2483
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Line	195	195
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Method k5_asn1_decode_int(const uint8_t *asn1, size_t len, intmax_t *val)

```
....
195.      if (len > sizeof(intmax_t) + (asn1[0] == 0))
```

Arithmenic Operation On Boolean\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2484
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.18.5-final-CVE-2020-28196-FP.c
Method k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2485
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.19.1-final-CVE-2020-28196-FP.c
Method k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20

	031&pathid=2486
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.19.2-final-CVE-2020-28196-FP.c
Method k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

Arithmenic Operation On Boolean\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2487
Status	New

	Source	Destination
File	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Line	214	214
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2020-28196-FP.c
Method k5_asn1_decode_uint(const uint8_t *asn1, size_t len, uintmax_t *val)

```
....
214.      if ((asn1[0] & 0x80) || len > sizeof(uintmax_t) + (asn1[0] ==
0))
```

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=1020038&projectid=20031&pathid=2488
Status	New

Method uECC_shared_secret in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1063	1063
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2489
Status	New

Method uECC_shared_secret in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1064	1064
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2490
Status	New

Method uECC_shared_secret in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1086	1086
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2491
Status	New

Method uECC_decompress in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1114	1114
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2492

Status	New

Method bits2int in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1224	1224
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2493
Status	New

Method uECC_sign_with_k_internal in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1306	1306
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2494
Status	New

Method uECC_sign_with_k_internal in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1322	1322
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2495
Status	New

Method uECC_verify in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1520	1520
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-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=1020038&projectid=20031&pathid=2496
Status	New

Method uECC_verify in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	1521	1521
Object	bcopy	bcopy

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Method int uECC_verify(const uint8_t *public_key,

```
....
1521.      bcopy((uint8_t *) s, signature + curve->num_bytes, curve->num_bytes);
```

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=1020038&projectid=20031&pathid=2098
Status	New

The buffer allocated by <= in iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c at line 927 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c	iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Line	953	953
Object	<=	<=

Code Snippet
File Name iovisor@@bcc-0.29.0-CVE-2021-3520-FP.c
Method void print_log2_hist(unsigned int *vals, int vals_size, const char *val_type)

```
....
953.        for (i = 0; i <= idx_max; 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=1020038&projectid=20031&pathid=2099
Status	New

The buffer allocated by <= in iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c at line 894 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	920	920
Object	<=	<=

Code Snippet
File Name iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method void print_log2_hist(unsigned int *vals, int vals_size, const char *val_type)

```
....
920.        for (i = 0; i <= idx_max; 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=1020038&projectid=20031&pathid=2100
Status	New

The buffer allocated by <= in iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c at line 894 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	920	920
Object	<=	<=

Code Snippet
File Name iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method void print_log2_hist(unsigned int *vals, int vals_size, const char *val_type)

```
....
920.        for (i = 0; i <= idx_max; 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=1020038&projectid=20031&pathid=2101
Status	New

The buffer allocated by <= in iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c at line 895 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Line	921	921
Object	<=	<=

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method void print_log2_hist(unsigned int *vals, int vals_size, const char *val_type)

```
....
921.        for (i = 0; i <= idx_max; 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=1020038&projectid=20031&pathid=2102
Status	New

The buffer allocated by <= in iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c at line 928 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Line	954	954
Object	<=	<=

Code Snippet
File Name iovisor@@bcc-v0.30.0-CVE-2021-3520-FP.c
Method void print_log2_hist(unsigned int *vals, int vals_size, const char *val_type)

```
....
954.        for (i = 0; i <= idx_max; 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=1020038&projectid=20031&pathid=2103
Status	New

The buffer allocated by <= in kmackay@@micro-ecc-v1.1-CVE-2020-27209-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	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c	kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Line	427	427
Object	<=	<=

Code Snippet
File Name kmackay@@micro-ecc-v1.1-CVE-2020-27209-FP.c
Method uECC_VLI_API void uECC_vli_mult(uECC_word_t *result,

```
....
427.          for (i = 0; i <= k; ++i) {
```

Heuristic Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic Buffer Overflow malloc Version:0

Categories

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

Description
Heuristic Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2474
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.21.0-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 create_tmp_vdso_image passes to f, at line 527 of iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Line	545	562
Object	f	sz

Code Snippet

File Name	iovisor@@bcc-v0.21.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
545.                ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
....
562.         image = malloc(sz);
```

Heuristic Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2475
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 527 of iovisor@@bcc-v0.23.0-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 create_tmp_vdso_image passes to f, at line 527 of iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Line	545	562
Object	f	sz

Code Snippet

File Name	iovisor@@bcc-v0.23.0-CVE-2021-3520-FP.c
Method	static int create_tmp_vdso_image(struct dso *dso)

```
....
545.                ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
....
562.         image = malloc(sz);
```

Heuristic Buffer Overflow malloc\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=2476
Status	New

The size of the buffer used by create_tmp_vdso_image in sz, at line 528 of iovisor@@bcc-v0.25.0-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 create_tmp_vdso_image passes to f, at line 528 of iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c	iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c

Line	546	563
Object	f	sz

Code Snippet
File Name iovisor@@bcc-v0.25.0-CVE-2021-3520-FP.c
Method static int create_tmp_vdso_image(struct dso *dso)

```
....
546.              ret = fscanf(f, "%lx-%lx %*s %*x %*x:%*x %*u%[^\n]",
....
563.        image = malloc(sz);
```

Potential Path Traversal

Query Path:
CPP\Cx\CPP Low Visibility\Potential Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description
Potential Path Traversal\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1925
Status	New

Method main at line 137 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in setoutput at line 597 of jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Line	137	607
Object	argv	filename

Code Snippet
File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

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

File Name jart@@cosmopolitan-3.3.1-CVE-2024-6381-TP.c
Method void setoutput(char *filename)

```
....
607.      outfile = fopen(filename, Hflag? "wb":"wt");
```

Potential Path Traversal\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1926
Status	New

Method main at line 137 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in setoutput at line 597 of jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c	jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Line	137	607
Object	argv	filename

Code Snippet
File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method int main(int argc, char **argv)

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

File Name jart@@cosmopolitan-3.5.0-CVE-2024-6381-TP.c
Method void setoutput(char *filename)

```
....
607.      outfile = fopen(filename, Hflag? "wb":"wt");
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020038&projectid=20031&pathid=1924
Status	New

	Source	Destination

File	krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.c	krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.c
Line	50	50
Object	getopt	getopt

Code Snippet
File Name krb5@@krb5-krb5-1.19.4-final-CVE-2022-42898-FP.c
Method main(int argc, char **argv)

```
....
50.      while ((c = getopt(argc, argv, "e:T:")) != -1) {
```

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

```
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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

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

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;
}
```

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;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

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());
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Potential Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
```

```
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

BACK TO TOP

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Heuristic 2nd Order Buffer Overflow malloc

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Heuristic Buffer Overflow malloc

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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 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)
    }
```

```
}
```

Insufficiently Protected Credentials

Risk

What might happen

An attacker could steal user credentials, enabling access to user accounts and confidential data.

Cause

How does it happen

User passwords are written to the database without being properly encrypted with a cryptographic hash. The application reads clear passwords straight from the database.

General Recommendations

How to avoid it

Store passwords using a cryptographic hash designed as a password protection scheme, such as:

- bcrypt
- scrypt
- PBKDF2 (with random salt) These need to be configured with an appropriately high work effort.

Source Code Examples

CSharp

Always use a secure password protection scheme to store passwords, such as bcrypt:

```
string hashed = BCrypt.HashPassword(password, BCrypt.GenerateSalt(12));
```

For password verification, use the matching function:

```
bool isValid = BCrypt.CheckPassword(candidate, hashed);
```

```

```

Java

Always use a secure password protection scheme to store passwords, such as bcrypt:

```
String hashed = BCrypt.hashpw(password, BCrypt.gensalt(12));
```

For password verification, use the matching function:

```
bool isValid = BCrypt.checkpw(candidate, hashed);
```

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

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