F-STACK-1 Scan Report

Project Name	F-STACK-1
Scan Start	Friday, June 21, 2024 4:28:21 PM
Preset	Checkmarx Default
Scan Time	03h:31m:55s
Lines Of Code Scanned	220883
Files Scanned	85
Report Creation Time	Friday, June 21, 2024 7:04:49 PM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	4/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

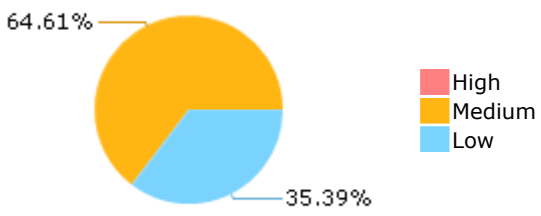
Results Limit

Results limit per query was set to 50

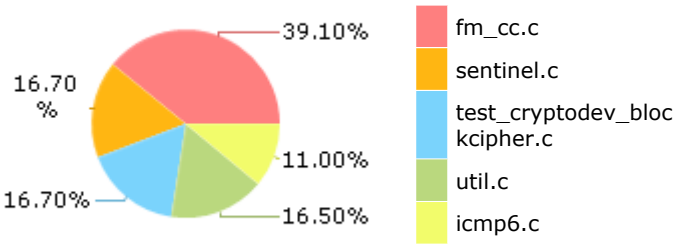
Selected Queries

Selected queries are listed in Result Summary

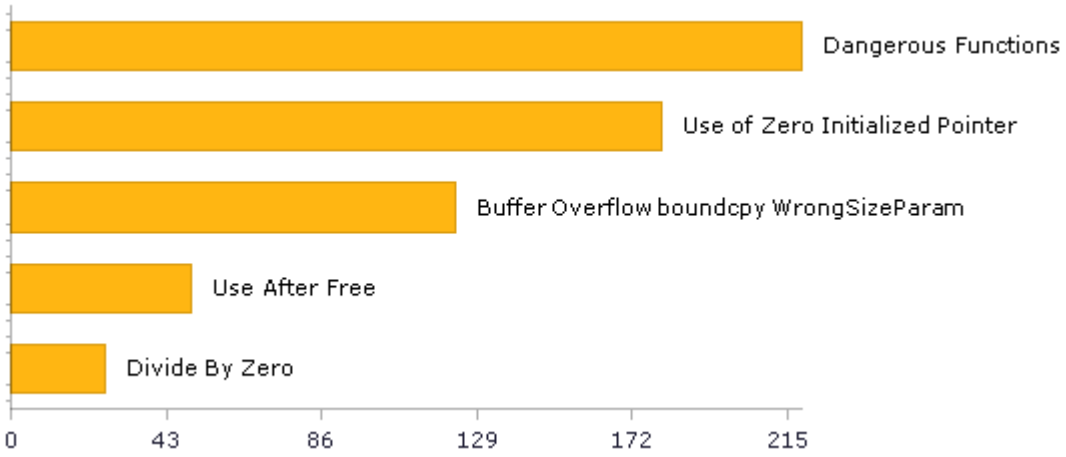
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	334	174
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	20	20
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	17	17
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	244	244
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	2	2
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	244	244
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	10	10
PCI DSS (3.2) - 6.5.2 - Buffer overflows	141	141
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.	4	4
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.	1	1
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	17	17
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.	17	17
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.	16	16

***** 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)	20	20
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)	16	16
SC-4 Information in Shared Resources (P1)	2	2
SC-5 Denial of Service Protection (P1)*	397	94
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	45	42
SI-11 Error Handling (P2)*	57	57
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	10	10

***** 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

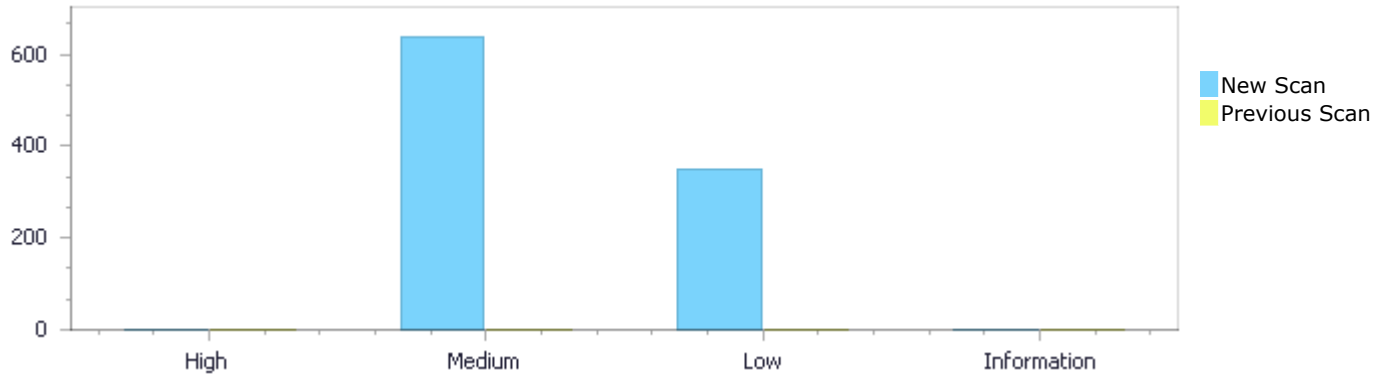
Scan Summary - Custom

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	0	639	350	0	989
Recurrent Issues	0	0	0	0	0
Total	0	639	350	0	989
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	0	639	350	0	989
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	639	350	0	989

Result Summary

Vulnerability Type	Occurrences	Severity
Dangerous Functions	219	Medium
Use of Zero Initialized Pointer	180	Medium
Buffer Overflow boundcpy WrongSizeParam	123	Medium
Use After Free	50	Medium
Divide By Zero	26	Medium

Integer Overflow	16	Medium
Use of Uninitialized Pointer	8	Medium
Use of Uninitialized Variable	6	Medium
Stored Buffer Overflow boundcpy	4	Medium
Char Overflow	2	Medium
Heap Inspection	2	Medium
Memory Leak	2	Medium
Wrong Size t Allocation	1	Medium
NULL Pointer Dereference	147	Low
Unchecked Return Value	57	Low
Use of Sizeof On a Pointer Type	34	Low
Use of Obsolete Functions	25	Low
Unchecked Array Index	23	Low
Improper Resource Access Authorization	16	Low
Use of Insufficiently Random Values	15	Low
Potential Off by One Error in Loops	10	Low
TOCTOU	8	Low
Sizeof Pointer Argument	6	Low
Incorrect Permission Assignment For Critical Resources	4	Low
Unreleased Resource Leak	3	Low
Arithmenic Operation On Boolean	1	Low
Information Exposure Through Comments	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
f-stack-2/fm_cc.c	174
f-stack-2/util.c	67
f-stack-2/test_cryptodev_blockcipher.c	53
f-stack-2/ngx_http_upstream.c	44
f-stack-2/t_stream.c	40
f-stack-2/sentinel.c	40
f-stack-2/sds.c	25
f-stack-2/ar9300_paprd.c	20
f-stack-2/aof.c	18
f-stack-2/db.c	14

Scan Results Details

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=180
Status	New

The dangerous function, memcpy, was found in use at line 125 in f-stack-2/aof.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	135	135
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/aof.c
Method void aofRewriteBufferAppend(unsigned char *s, unsigned long len) {

```
....
135.                    memcpy(block->buf+block->used, s, thislen);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=181
Status	New

The dangerous function, memcpy, was found in use at line 593 in f-stack-2/bitops.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	676	676

Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/bitops.c
Method void bitopCommand(client *c) {

```
....
676.                memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=182
Status	New

The dangerous function, memcpy, was found in use at line 593 in f-stack-2/bitops.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	677	677
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/bitops.c
Method void bitopCommand(client *c) {

```
....
677.                memcpy(res,src[0],minlen);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=183
Status	New

The dangerous function, memcpy, was found in use at line 467 in f-stack-2/db.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	481	481
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/db.c
Method dbBackup *backupDb(void) {

```
....
481.          memcpy(backup->slots_keys_count, server.cluster-
>slots_keys_count,
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=184
Status	New

The dangerous function, memcpy, was found in use at line 523 in f-stack-2/db.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	538	538
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/db.c
Method void restoreDbBackup(dbBackup *buckup) {

```
....
538.          memcpy(server.cluster->slots_keys_count, buckup-
>slots_keys_count,
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=185
Status	New

The dangerous function, memcpy, was found in use at line 1575 in f-stack-2/db.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1592	1592
Object	memcpy	memcpy

Code Snippet

File Name	f-stack-2/db.c
Method	int *getKeysPrepareResult(getKeysResult *result, int numkeys) {

```
....
1592.                   memcpy(result->keys, result->keysbuf, result-
>numkeys * sizeof(int));
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=186
Status	New

The dangerous function, memcpy, was found in use at line 1916 in f-stack-2/db.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1926	1926
Object	memcpy	memcpy

Code Snippet	
File Name	f-stack-2/db.c
Method	void slotToKeyUpdateKey(sds key, int add) {

```
....
1926.       memcpy(indexed+2,key,keylen);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=187
Status	New

The dangerous function, memcpy, was found in use at line 40 in f-stack-2/enic_rxtx_vec_avx2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/enic_rxtx_vec_avx2.c	f-stack-2/enic_rxtx_vec_avx2.c
Line	787	787
Object	memcpy	memcpy

Code Snippet	
File Name	f-stack-2/enic_rxtx_vec_avx2.c
Method	enic_noscatter_vec_recv_pkts(void *rx_queue, struct rte_mbuf **rx_pkts,

```
....
787.        memcpy(rxmb, rq->free_mbufs + ENIC_RX_BURST_MAX - rq-
>num_free_mbufs,
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=188
Status	New

The dangerous function, memcpy, was found in use at line 593 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	808	808
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error ReleaseModifiedDataStructure(

```
....
808.          memcpy(((t_FmPcdCcNode *)(p_AdditionalParams-
>h_CurrentNode))->keyAndNextEngineParams,
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=189
Status	New

The dangerous function, memcpy, was found in use at line 593 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	821	821
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error ReleaseModifiedDataStructure(

```
....
821.          memcpy(&((t_FmPcdCcTree *)(p_AdditionalParams-
>h_CurrentNode))->keyAndNextEngineParams,
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=190
Status	New

The dangerous function, memcpy, was found in use at line 2377 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2400	2400
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error UpdateGblMask(t_FmPcdCcNode *p_CcNode, uint8_t keySize,

```
....
2400.              memcpy(p_CcNode->p_GlblMask, p_Mask,
(sizeof(uint8_t)) * keySize);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=191
Status	New

The dangerous function, memcpy, was found in use at line 2566 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2599	2599
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2599.       memcpy(&p_AdditionalInfo-
>keyAndNextEngineParams[keyIndex].nextEngineParams,
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=192
Status	New

The dangerous function, memcpy, was found in use at line 2566 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2602	2602
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2602.       memcpy(p_AdditionalInfo-
>keyAndNextEngineParams[keyIndex].key,
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=193
Status	New

The dangerous function, memcpy, was found in use at line 2566 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2617	2617
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2617.          memcpy(p_AdditionalInfo-
>keyAndNextEngineParams[keyIndex].mask,
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=194
Status	New

The dangerous function, memcpy, was found in use at line 2940 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2962	2962
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeModifyKey(

```
....
2962.      memcpy(p_AdditionalInfo-
>keyAndNextEngineParams[keyIndex].key, p_Key,
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=195
Status	New

The dangerous function, memcpy, was found in use at line 2940 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2966	2966
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeModifyKey(

```
....
2966.          memcpy(p_AdditionalInfo-
>keyAndNextEngineParams[keyIndex].mask, p_Mask,
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=196
Status	New

The dangerous function, memcpy, was found in use at line 3094 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3124	3124
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3124.      memcpy(&p_AdditionalInfo-
>keyAndNextEngineParams[keyIndex].nextEngineParams,
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=197
Status	New

The dangerous function, memcpy, was found in use at line 3429 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3457	3457
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

```
....
3457.          memcpy(p_KeyAndNextEngineParams, p_CcNode-
>keyAndNextEngineParams,
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=198
Status	New

The dangerous function, memcpy, was found in use at line 3429 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3494	3494
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

```
....
3494.          memcpy(p_KeyAndNextEngineParams,
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=199
Status	New

The dangerous function, memcpy, was found in use at line 3429 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3528	3528
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

```
....
3528.              memcpy(&p_FmPcdModifyCcKeyAdditionalParams-
>keyAndNextEngineParams[j],
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=200
Status	New

The dangerous function, memcpy, was found in use at line 3429 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3542	3542
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

```
....
3542.      memcpy(&p_FmPcdModifyCcKeyAdditionalParams-
>keyAndNextEngineParams[j],
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=201
Status	New

The dangerous function, memcpy, was found in use at line 3705 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3737	3737
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error CheckParams(t_Handle h_FmPcd, t_FmPcdCcNodeParams *p_CcNodeParam,

```
....
3737.      memcpy(&p_CcNode->keyAndNextEngineParams[p_CcNode-
>numOfKeys].nextEngineParams,
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=202
Status	New

The dangerous function, memcpy, was found in use at line 3705 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3782	3782
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error CheckParams(t_Handle h_FmPcd, t_FmPcdCcNodeParams *p_CcNodeParam,

```
....
3782.          memcpy(p_CcNode->keyAndNextEngineParams[tmp].key,
p_KeyParams->p_Key,
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=203
Status	New

The dangerous function, memcpy, was found in use at line 3705 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3786	3786
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c

Method	static t_Error CheckParams(t_Handle h_FmPcd, t_FmPcdCcNodeParams *p_CcNodeParam,

```
....
3786.               memcpy(p_CcNode->keyAndNextEngineParams[tmp].mask,
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=204
Status	New

The dangerous function, memcpy, was found in use at line 3705 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3793	3793
Object	memcpy	memcpy

Code Snippet	
File Name	f-stack-2/fm_cc.c
Method	static t_Error CheckParams(t_Handle h_FmPcd, t_FmPcdCcNodeParams *p_CcNodeParam,

```
....
3793.           memcpy(&p_CcNode-
>keyAndNextEngineParams[tmp].nextEngineParams,
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=205
Status	New

The dangerous function, memcpy, was found in use at line 3825 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3871	3871
Object	memcpy	memcpy

Code Snippet	
File Name	f-stack-2/fm_cc.c

Method	static t_Error Ipv4TtlOrIpv6HopLimitCheckParams(

```
....
3871.       memcpy(&p_CcNode->keyAndNextEngineParams[p_CcNode-
>numOfKeys].nextEngineParams,
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=206
Status	New

The dangerous function, memcpy, was found in use at line 3825 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3924	3924
Object	memcpy	memcpy

Code Snippet	
File Name	f-stack-2/fm_cc.c
Method	static t_Error Ipv4TtlOrIpv6HopLimitCheckParams(

```
....
3924.           memcpy(&p_CcNode-
>keyAndNextEngineParams[tmp].nextEngineParams,
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=207
Status	New

The dangerous function, memcpy, was found in use at line 3946 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4034	4034
Object	memcpy	memcpy

Code Snippet	
File Name	f-stack-2/fm_cc.c
Method	static t_Error IcHashIndexedCheckParams(t_Handle h_FmPcd,

```
....
4034.              memcpy(&p_CcNode-
>keyAndNextEngineParams[tmp].nextEngineParams,
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=208
Status	New

The dangerous function, memcpy, was found in use at line 3946 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4064	4064
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error IcHashIndexedCheckParams(t_Handle h_FmPcd,

```
....
4064.      memcpy(PTR_MOVE(p_CcNode->p_GlblMask, 2), &glblMask, 2);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=209
Status	New

The dangerous function, memcpy, was found in use at line 4938 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4950	4950
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method void EnqueueNodeInfoToRelevantLst(t_List *p_List, t_CcNodeInformation *p_CcInfo,

```
....
4950.          memcpy(p_CcInformation, p_CcInfo,
sizeof(t_CcNodeInformation));
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=210
Status	New

The dangerous function, memcpy, was found in use at line 5994 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6103	6103
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6103.          memcpy(netEnvParams.unitIds, &p_FmPcdCcGroupParams-
>unitIds,
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=211
Status	New

The dangerous function, memcpy, was found in use at line 5994 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6146	6146
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6146.               memcpy(&p_KeyAndNextEngineParams->nextEngineParams,
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=212
Status	New

The dangerous function, memcpy, was found in use at line 5994 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6202	6202
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6202.           memcpy(&p_FmPcdCcTree->keyAndNextEngineParams[i],
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=213
Status	New

The dangerous function, memcpy, was found in use at line 6908 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6927	6927
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FM_PCD_MatchTableGetNextEngine(

```
....
6927.       memcpy(p_FmPcdCcNextEngineParams,
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=214
Status	New

The dangerous function, memcpy, was found in use at line 7073 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	7091	7091
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FM_PCD_MatchTableGetIndexedHashBucket(t_Handle h_CcNode,

```
....
7091.       memcpy(&glblMask, PTR_MOVE(p_CcNode->p_GlblMask, 2), 2);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=215
Status	New

The dangerous function, memcpy, was found in use at line 7489 in f-stack-2/fm_cc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	7502	7502
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FM_PCD_HashTableGetMissNextEngine(

```
....
7502.       memcpy(p_FmPcdCcNextEngineParams,
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=216
Status	New

The dangerous function, memcpy, was found in use at line 384 in f-stack-2/listpack.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/listpack.c	f-stack-2/listpack.c
Line	387	387
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/listpack.c
Method void lpEncodeString(unsigned char *buf, unsigned char *s, uint32_t len) {

```
....
387.            memcpy(buf+1,s,len);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=217
Status	New

The dangerous function, memcpy, was found in use at line 384 in f-stack-2/listpack.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/listpack.c	f-stack-2/listpack.c
Line	391	391
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/listpack.c
Method void lpEncodeString(unsigned char *buf, unsigned char *s, uint32_t len) {

```
....
391.          memcpy(buf+2,s,len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=218
Status	New

The dangerous function, memcpy, was found in use at line 384 in f-stack-2/listpack.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/listpack.c	f-stack-2/listpack.c
Line	398	398
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/listpack.c
Method void lpEncodeString(unsigned char *buf, unsigned char *s, uint32_t len) {

```
....
398.          memcpy(buf+5,s,len);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=219
Status	New

The dangerous function, memcpy, was found in use at line 655 in f-stack-2/listpack.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/listpack.c	f-stack-2/listpack.c
Line	753	753
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/listpack.c
Method unsigned char *lpInsert(unsigned char *lp, unsigned char *ele, uint32_t size, unsigned char *p, int where, unsigned char **newp) {

```
....
753.              memcpy(dst,intenc,enclen);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=220
Status	New

The dangerous function, memcpy, was found in use at line 655 in f-stack-2/listpack.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/listpack.c	f-stack-2/listpack.c
Line	758	758
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/listpack.c
Method unsigned char *lpInsert(unsigned char *lp, unsigned char *ele, uint32_t size, unsigned char *p, int where, unsigned char **newp) {

```
....
758.          memcpy(dst,backlen,backlen_size);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=221
Status	New

The dangerous function, memcpy, was found in use at line 293 in f-stack-2/lua_struct.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/lua_struct.c	f-stack-2/lua_struct.c
Line	325	325
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/lua_struct.c
Method static int b_unpack (lua_State *L) {

```
....
325.          memcpy(&f, data+pos, size);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=222
Status	New

The dangerous function, memcpy, was found in use at line 293 in f-stack-2/lua_struct.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/lua_struct.c	f-stack-2/lua_struct.c
Line	332	332
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/lua_struct.c
Method static int b_unpack (lua_State *L) {

```
....
332.          memcpy(&d, data+pos, size);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=223
Status	New

The dangerous function, memcpy, was found in use at line 294 in f-stack-2/lvm.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/lvm.c	f-stack-2/lvm.c
Line	325	325
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/lvm.c
Method void luaV_concat (lua_State *L, int total) {

```
....
325.          memcpy(buffer+tl, svalue(top-i), l * sizeof(char));
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=224
Status	New

The dangerous function, memcpy, was found in use at line 58 in f-stack-2/multi.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/multi.c	f-stack-2/multi.c
Line	75	75
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/multi.c
Method void queueMultiCommand(client *c) {

```
....
75.      memcpy(mc->argv,c->argv,sizeof(robj*)*c->argc);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=225
Status	New

The dangerous function, memcpy, was found in use at line 2027 in f-stack-2/ngx_string.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/ngx_string.c	f-stack-2/ngx_string.c
Line	2034	2034
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/ngx_string.c
Method ngx_memcpy(void *dst, const void *src, size_t n)

```
....
2034.       return memcpy(dst, src, n);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=226
Status	New

The dangerous function, memcpy, was found in use at line 103 in f-stack-2/sds.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	163	163
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/sds.c
Method sds _sdsnewlen(const void *init, size_t initlen, int trymalloc) {

```
....
163.           memcpy(s, init, initlen);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=227
Status	New

The dangerous function, memcpy, was found in use at line 233 in f-stack-2/sds.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	271	271
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/sds.c
Method sds sdsMakeRoomFor(sds s, size_t addlen) {

```
....
271.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=228
Status	New

The dangerous function, memcpy, was found in use at line 290 in f-stack-2/sds.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	317	317
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/sds.c
Method sds sdsRemoveFreeSpace(sds s) {

```
....
317.          memcpy((char*)newsh+hdrlen, s, len+1);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=229
Status	New

The dangerous function, memcpy, was found in use at line 432 in f-stack-2/sds.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	437	437
Object	memcpy	memcpy

Code Snippet
File Name f-stack-2/sds.c
Method sds sdscatlen(sds s, const void *t, size_t len) {

```
....
437.      memcpy(s+curlen, t, len);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=467
Status	New

The variable declared in p at f-stack-2/bitops.c in line 508 is not initialized when it is used by src at f-stack-2/bitops.c in line 934.

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	510	1123
Object	p	src

Code Snippet
File Name f-stack-2/bitops.c
Method unsigned char *getObjectReadOnlyString(robj *o, long *len, char *llbuf) {

```
....
510.      unsigned char *p = NULL;
```

File Name f-stack-2/bitops.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
1123.                  src = getObjectReadOnlyString(o,&strlen,llbuf);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=468
Status	New

The variable declared in src at f-stack-2/bitops.c in line 934 is not initialized when it is used by src at f-stack-2/bitops.c in line 934.

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	1119	1134
Object	src	src

Code Snippet
File Name f-stack-2/bitops.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
1119.              unsigned char *src = NULL;
....
1134.                  buf[i] = src[i+byte];
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=469
Status New

The variable declared in ops at f-stack-2/bitops.c in line 934 is not initialized when it is used by ops at f-stack-2/bitops.c in line 934.

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	938	1001
Object	ops	ops

Code Snippet
File Name f-stack-2/bitops.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
938.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
1001.           ops = zrealloc(ops,sizeof(*ops)*(numops+1));
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=470
Status New

The variable declared in ops at f-stack-2/bitops.c in line 934 is not initialized when it is used by ops at f-stack-2/bitops.c in line 934.

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	938	1001
Object	ops	ops

Code Snippet
File Name f-stack-2/bitops.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
938.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
1001.          ops = zrealloc(ops,sizeof(*ops)*(numops+1));
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=471
Status New

The variable declared in ops at f-stack-2/bitops.c in line 934 is not initialized when it is used by ops at f-stack-2/bitops.c in line 934.

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	938	1041
Object	ops	ops

Code Snippet
File Name f-stack-2/bitops.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
938.      struct bitfieldOp *ops = NULL; /* Array of ops to execute at
end. */
....
1041.          struct bitfieldOp *thisop = ops+j;
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=300

	36&pathid=472
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4819	107
Object	p_StatsObj	p_StatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4819.           p_CcNode->keyAndNextEngineParams[tmp].p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.           p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=473
Status	New

The variable declared in p_GlblMask at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1243	107
Object	p_GlblMask	p_StatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1243.           p_CcNode->p_GlblMask = NULL;
```

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.          p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=474
Status	New

The variable declared in h_Ad at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1264	107
Object	h_Ad	p_StatsObj

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1264.           p_CcNode->h_Ad = NULL;
```

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.          p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=475
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4776	107
Object	p_StatsObj	p_StatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4776.              p_CcNode->keyAndNextEngineParams[tmp].p_StatsObj =
NULL;
```

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.          p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=476
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 99 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	101	107
Object	p_StatsObj	p_StatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
101.      t_FmPcdStatsObj *p_StatsObj = NULL;
....
107.          p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=477
Status	New

The variable declared in h_StatsFLRs at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1272	107
Object	h_StatsFLRs	p_StatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1272.           p_CcNode->h_StatsFLRs = NULL;
```

File Name f-stack-2/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.           p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=478
Status	New

The variable declared in h_Spinlock at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1278	107
Object	h_Spinlock	p_StatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1278.           p_CcNode->h_Spinlock = NULL;
```

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.           p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=479
Status	New

The variable declared in h_AdTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1257	107
Object	h_AdTable	p_StatsObj

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1257.           p_CcNode->h_AdTable = NULL;
```

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.           p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=480

Status	New

The variable declared in h_KeysMatchTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at f-stack-2/fm_cc.c in line 99.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1250	107
Object	h_KeysMatchTable	p_StatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1250.           p_CcNode->h_KeysMatchTable = NULL;
```

File Name f-stack-2/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
107.           p_StatsObj = NCSW_LIST_OBJECT(p_Next, t_FmPcdStatsObj,
node);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=481
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by p_CcNodeInfo at f-stack-2/fm_cc.c in line 1202.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4819	1209
Object	p_StatsObj	p_CcNodeInfo

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4819.           p_CcNode->keyAndNextEngineParams[tmp].p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_CcNodeInformation * DequeueAdditionalInfoFromRelevantLst(

```
....
1209.          p_CcNodeInfo = CC_NODE_F_OBJECT(p_List->p_Next);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=482
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 99 is not initialized when it is used by p_CcNodeInfo at f-stack-2/fm_cc.c in line 1202.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	101	1209
Object	p_StatsObj	p_CcNodeInfo

Code Snippet

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
101.      t_FmPcdStatsObj *p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_CcNodeInformation * DequeueAdditionalInfoFromRelevantLst(

```
....
1209.          p_CcNodeInfo = CC_NODE_F_OBJECT(p_List->p_Next);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=483
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by p_CcNodeInfo at f-stack-2/fm_cc.c in line 1202.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4776	1209
Object	p_StatsObj	p_CcNodeInfo

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4776.              p_CcNode->keyAndNextEngineParams[tmp].p_StatsObj =
NULL;
```

File Name f-stack-2/fm_cc.c
Method static t_CcNodeInformation * DequeueAdditionalInfoFromRelevantLst(

```
....
1209.          p_CcNodeInfo = CC_NODE_F_OBJECT(p_List->p_Next);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=484
Status	New

The variable declared in p_GlblMask at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_CcNodeInfo at f-stack-2/fm_cc.c in line 1202.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1243	1209
Object	p_GlblMask	p_CcNodeInfo

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1243.          p_CcNode->p_GlblMask = NULL;
```

File Name f-stack-2/fm_cc.c
Method static t_CcNodeInformation * DequeueAdditionalInfoFromRelevantLst(

```
....
1209.          p_CcNodeInfo = CC_NODE_F_OBJECT(p_List->p_Next);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=485
Status	New

The variable declared in h_KeysMatchTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_CcNodeInfo at f-stack-2/fm_cc.c in line 1202.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1250	1209
Object	h_KeysMatchTable	p_CcNodeInfo

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1250.          p_CcNode->h_KeysMatchTable = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_CcNodeInformation * DequeueAdditionalInfoFromRelevantLst(

```
....
1209.          p_CcNodeInfo = CC_NODE_F_OBJECT(p_List->p_Next);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=486
Status	New

The variable declared in p_CcNodeInfo at f-stack-2/fm_cc.c in line 1202 is not initialized when it is used by p_CcNodeInfo at f-stack-2/fm_cc.c in line 1216.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1205	1222

Object	p_CcNodeInfo	p_CcNodeInfo

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_CcNodeInformation * DequeueAdditionalInfoFromRelevantLst(

```
....
1205.      t_CcNodeInformation *p_CcNodeInfo = NULL;
```

File Name f-stack-2/fm_cc.c

Method void ReleaseLst(t_List *p_List)

```
....
1222.          p_CcNodeInfo =
DequeueAdditionalInfoFromRelevantLst(p_List);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=487
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	101	2211
Object	p_StatsObj	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
101.      t_FmPcdStatsObj *p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2211.          p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=488
Status	New

The variable declared in p_AdTableNew at f-stack-2/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2519	2211
Object	p_AdTableNew	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static t_Error BuildNewNodeCommonPart(

```
....
2519.               p_AdditionalInfo->p_AdTableNew = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2211.           p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=489
Status	New

The variable declared in h_Ad at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1264	2211
Object	h_Ad	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1264.          p_CcNode->h_Ad = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2211.          p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=490
Status	New

The variable declared in h_KeysMatchTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1250	2211
Object	h_KeysMatchTable	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1250.          p_CcNode->h_KeysMatchTable = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2211.          p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=491
Status	New

The variable declared in p_GlblMask at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1243	2211
Object	p_GlblMask	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1243.           p_CcNode->p_GlblMask = NULL;
```

File Name f-stack-2/fm_cc.c
Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2211.           p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=492
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	101	308
Object	p_StatsObj	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
101.       t_FmPcdStatsObj *p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
308.          p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=493
Status	New

The variable declared in p_AdTableNew at f-stack-2/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2519	308
Object	p_AdTableNew	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeCommonPart(

```
....
2519.              p_AdditionalInfo->p_AdTableNew = NULL;
```

File Name f-stack-2/fm_cc.c
Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
308.          p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=494
Status	New

The variable declared in h_Ad at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c

Line	1264	308
Object	h_Ad	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1264.           p_CcNode->h_Ad = NULL;
```

File Name f-stack-2/fm_cc.c
Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
308.           p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=495
Status	New

The variable declared in h_KeysMatchTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1250	308
Object	h_KeysMatchTable	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1250.           p_CcNode->h_KeysMatchTable = NULL;
```

File Name f-stack-2/fm_cc.c
Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
308.           p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=496
Status	New

The variable declared in p_GlblMask at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1243	308
Object	p_GlblMask	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1243.           p_CcNode->p_GlblMask = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
308.            p_AdNewPtr = h_Ad;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=497
Status	New

The variable declared in h_TmpAd at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_KeysMatchTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1265	4707
Object	h_TmpAd	h_KeysMatchTable

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1265.          p_CcNode->h_TmpAd = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4707.          MemSet8((uint8_t *)p_CcNode->h_KeysMatchTable, 0,
matchTableSize);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=498
Status	New

The variable declared in h_KeysMatchTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_KeysMatchTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1250	4707
Object	h_KeysMatchTable	h_KeysMatchTable

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1250.          p_CcNode->h_KeysMatchTable = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4707.          MemSet8((uint8_t *)p_CcNode->h_KeysMatchTable, 0,
matchTableSize);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=499

Status	New

The variable declared in h_AdTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_KeysMatchTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1257	4707
Object	h_AdTable	h_KeysMatchTable

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1257.           p_CcNode->h_AdTable = NULL;
```

File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4707.           MemSet8((uint8_t *)p_CcNode->h_KeysMatchTable, 0,
matchTableSize);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=500
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 99 is not initialized when it is used by h_KeysMatchTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	101	4707
Object	p_StatsObj	h_KeysMatchTable

Code Snippet
File Name f-stack-2/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
101.      t_FmPcdStatsObj *p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4707.          MemSet8((uint8_t *)p_CcNode->h_KeysMatchTable, 0,
matchTableSize);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=501
Status	New

The variable declared in p_AdTableNew at f-stack-2/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2519	2198
Object	p_AdTableNew	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static t_Error BuildNewNodeCommonPart(

```
....
2519.              p_AdditionalInfo->p_AdTableNew = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2198.      p_AdNewPtr = p_AdResult;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=502
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	101	2198
Object	p_StatsObj	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
101.      t_FmPcdStatsObj *p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c
Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2198.      p_AdNewPtr = p_AdResult;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=503
Status	New

The variable declared in p_GlblMask at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1243	2198
Object	p_GlblMask	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1243.          p_CcNode->p_GlblMask = NULL;
```

File Name f-stack-2/fm_cc.c
Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2198.       p_AdNewPtr = p_AdResult;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=504
Status	New

The variable declared in h_Ad at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1264	2198
Object	h_Ad	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1264.           p_CcNode->h_Ad = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2198.       p_AdNewPtr = p_AdResult;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=505
Status	New

The variable declared in h_Spinlock at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 2169.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1278	2198

Object	h_Spinlock	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1278.          p_CcNode->h_Spinlock = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

```
....
2198.      p_AdNewPtr = p_AdResult;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=506
Status	New

The variable declared in p_AdTableNew at f-stack-2/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2519	295
Object	p_AdTableNew	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeCommonPart(

```
....
2519.              p_AdditionalInfo->p_AdTableNew = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
295.       p_AdNewPtr = p_AdContLookup;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=507
Status	New

The variable declared in p_StatsObj at f-stack-2/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	101	295
Object	p_StatsObj	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

```
....
101.      t_FmPcdStatsObj *p_StatsObj = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
295.      p_AdNewPtr = p_AdContLookup;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=508
Status	New

The variable declared in p_GlblMask at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1243	295
Object	p_GlblMask	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1243.          p_CcNode->p_GlblMask = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
295.       p_AdNewPtr = p_AdContLookup;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=509
Status	New

The variable declared in h_Ad at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1264	295
Object	h_Ad	p_AdNewPtr

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1264.          p_CcNode->h_Ad = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
295.       p_AdNewPtr = p_AdContLookup;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=510
Status	New

The variable declared in h_Spinlock at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at f-stack-2/fm_cc.c in line 266.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1278	295
Object	h_Spinlock	p_AdNewPtr

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1278.           p_CcNode->h_Spinlock = NULL;
```

File Name f-stack-2/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

```
....
295.       p_AdNewPtr = p_AdContLookup;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=511
Status	New

The variable declared in h_AdTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1257	4719
Object	h_AdTable	h_AdTable

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1257.           p_CcNode->h_AdTable = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4719.       MemSet8((uint8_t *)p_CcNode->h_AdTable, 0, adTableSize);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=512
Status	New

The variable declared in h_StatsFLRs at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1272	4719
Object	h_StatsFLRs	h_AdTable

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1272.           p_CcNode->h_StatsFLRs = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4719.       MemSet8((uint8_t *)p_CcNode->h_AdTable, 0, adTableSize);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=513
Status	New

The variable declared in h_Ad at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c

Line	1264	4719
Object	h_Ad	h_AdTable

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1264.          p_CcNode->h_Ad = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4719.      MemSet8((uint8_t *)p_CcNode->h_AdTable, 0, adTableSize);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=514
Status	New

The variable declared in h_KeysMatchTable at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1250	4719
Object	h_KeysMatchTable	h_AdTable

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1250.          p_CcNode->h_KeysMatchTable = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4719.      MemSet8((uint8_t *)p_CcNode->h_AdTable, 0, adTableSize);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=515
Status	New

The variable declared in p_GlblMask at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1243	4719
Object	p_GlblMask	h_AdTable

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1243.          p_CcNode->p_GlblMask = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4719.      MemSet8((uint8_t *)p_CcNode->h_AdTable, 0, adTableSize);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=516
Status	New

The variable declared in h_TmpAd at f-stack-2/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at f-stack-2/fm_cc.c in line 4324.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	1265	4719
Object	h_TmpAd	h_AdTable

Code Snippet

File Name f-stack-2/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

```
....
1265.          p_CcNode->h_TmpAd = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4719.      MemSet8((uint8_t *)p_CcNode->h_AdTable, 0, adTableSize);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=37
Status	New

The size of the buffer used by *backupDb in ->, at line 467 of f-stack-2/db.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *backupDb passes to ->, at line 467 of f-stack-2/db.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	482	482
Object	->	->

Code Snippet
File Name f-stack-2/db.c
Method dbBackup *backupDb(void) {

```
....
482.              sizeof(server.cluster->slots_keys_count));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=38
Status	New

The size of the buffer used by restoreDbBackup in ->, at line 523 of f-stack-2/db.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that restoreDbBackup passes to ->, at line 523 of f-stack-2/db.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	539	539
Object	->	->

Code Snippet
File Name f-stack-2/db.c
Method void restoreDbBackup(dbBackup *buckup) {

```
....
539.                    sizeof(server.cluster->slots_keys_count));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=39
Status New

The size of the buffer used by BuildNewNodeAddOrMdfyKeyAndNextEngine in t_FmPcdCcNextEngineParams, at line 2566 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BuildNewNodeAddOrMdfyKeyAndNextEngine passes to t_FmPcdCcNextEngineParams, at line 2566 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2600	2600
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2600.               &p_KeyParams->ccNextEngineParams,
sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=40
Status New

The size of the buffer used by BuildNewNodeModifyNextEngine in t_FmPcdCcNextEngineParams, at line 3094 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BuildNewNodeModifyNextEngine passes to t_FmPcdCcNextEngineParams, at line 3094 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3125	3125
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3125.              p_CcNextEngineParams,
sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=41
Status New

The size of the buffer used by ModifyNodeCommonPart in t_FmPcdCcKeyAndNextEngineParams, at line 3429 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ModifyNodeCommonPart passes to t_FmPcdCcKeyAndNextEngineParams, at line 3429 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3530	3530
Object	t_FmPcdCcKeyAndNextEngineParams	t_FmPcdCcKeyAndNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

```
....
3530.                       sizeof(t_FmPcdCcKeyAndNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=42
Status New

The size of the buffer used by ModifyNodeCommonPart in t_FmPcdCcKeyAndNextEngineParams, at line 3429 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ModifyNodeCommonPart passes to t_FmPcdCcKeyAndNextEngineParams, at line 3429 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3544	3544
Object	t_FmPcdCcKeyAndNextEngineParams	t_FmPcdCcKeyAndNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

```
....
3544.             sizeof(t_FmPcdCcKeyAndNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=43
Status New

The size of the buffer used by CheckParams in t_FmPcdCcNextEngineParams, at line 3705 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CheckParams passes to t_FmPcdCcNextEngineParams, at line 3705 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3739	3739
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error CheckParams(t_Handle h_FmPcd, t_FmPcdCcNodeParams *p_CcNodeParam,

```
....
3739.             sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=44
Status New

The size of the buffer used by CheckParams in t_FmPcdCcNextEngineParams, at line 3705 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CheckParams passes to t_FmPcdCcNextEngineParams, at line 3705 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3795	3795
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error CheckParams(t_Handle h_FmPcd, t_FmPcdCcNodeParams *p_CcNodeParam,

```
....
3795.                   sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=45
Status New

The size of the buffer used by Ipv4TtlOrIpv6HopLimitCheckParams in t_FmPcdCcNextEngineParams, at line 3825 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Ipv4TtlOrIpv6HopLimitCheckParams passes to t_FmPcdCcNextEngineParams, at line 3825 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3873	3873
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error Ipv4TtlOrIpv6HopLimitCheckParams(

```
....
3873.               sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=46
Status New

The size of the buffer used by Ipv4TtlOrIpv6HopLimitCheckParams in t_FmPcdCcNextEngineParams, at line 3825 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Ipv4TtlOrIpv6HopLimitCheckParams passes to t_FmPcdCcNextEngineParams, at line 3825 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3926	3926
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error Ipv4TtlOrIpv6HopLimitCheckParams(

```
....
3926.                   sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=47
Status New

The size of the buffer used by IcHashIndexedCheckParams in t_FmPcdCcNextEngineParams, at line 3946 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IcHashIndexedCheckParams passes to t_FmPcdCcNextEngineParams, at line 3946 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4036	4036
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error IcHashIndexedCheckParams(t_Handle h_FmPcd,

```
....
4036.                       sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=48
Status New

The size of the buffer used by EnqueueNodeInfoToRelevantLst in t_CcNodeInformation, at line 4938 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EnqueueNodeInfoToRelevantLst passes to t_CcNodeInformation, at line 4938 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4950	4950
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method void EnqueueNodeInfoToRelevantLst(t_List *p_List, t_CcNodeInformation *p_CcInfo,

```
....
4950.          memcpy(p_CcInformation, p_CcInfo,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=49
Status New

The size of the buffer used by FM_PCD_CcRootBuild in t_FmPcdCcNextEngineParams, at line 5994 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_CcRootBuild passes to t_FmPcdCcNextEngineParams, at line 5994 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6148	6148
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6148.                       sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=50
Status New

The size of the buffer used by FM_PCD_CcRootBuild in t_FmPcdCcKeyAndNextEngineParams, at line 5994 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_CcRootBuild passes to t_FmPcdCcKeyAndNextEngineParams, at line 5994 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6204	6204
Object	t_FmPcdCcKeyAndNextEngineParams	t_FmPcdCcKeyAndNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6204.                   sizeof(t_FmPcdCcKeyAndNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=51
Status New

The size of the buffer used by FM_PCD_MatchTableGetNextEngine in t_FmPcdCcNextEngineParams, at line 6908 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_MatchTableGetNextEngine passes to t_FmPcdCcNextEngineParams, at line 6908 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6929	6929
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FM_PCD_MatchTableGetNextEngine(

```
....
6929.               sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=52
Status New

The size of the buffer used by FM_PCD_HashTableGetMissNextEngine in t_FmPcdCcNextEngineParams, at line 7489 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_HashTableGetMissNextEngine passes to t_FmPcdCcNextEngineParams, at line 7489 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	7504	7504
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FM_PCD_HashTableGetMissNextEngine(

```
....
7504.              sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=53
Status New

The size of the buffer used by streamEncodeID in e, at line 371 of f-stack-2/t_stream.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streamEncodeID passes to e, at line 371 of f-stack-2/t_stream.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/t_stream.c	f-stack-2/t_stream.c
Line	375	375
Object	e	e

Code Snippet
File Name f-stack-2/t_stream.c
Method void streamEncodeID(void *buf, streamID *id) {

```
....
375.       memcpy(buf,e,sizeof(e));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=54
Status New

The size of the buffer used by ulp_mapper_field_src_process in uint32_t, at line 1015 of f-stack-2/ulp_mapper.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that ulp_mapper_field_src_process passes to uint32_t, at line 1015 of f-stack-2/ulp_mapper.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/ulp_mapper.c	f-stack-2/ulp_mapper.c
Line	1129	1129
Object	uint32_t	uint32_t

Code Snippet
File Name f-stack-2/ulp_mapper.c
Method ulp_mapper_field_src_process(struct bnxt_ulp_mapper_parms *parms,

```
....
1129.                    sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=55
Status New

The size of the buffer used by *backupDb in ->, at line 467 of f-stack-2/db.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *backupDb passes to ->, at line 467 of f-stack-2/db.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	485	485
Object	->	->

Code Snippet
File Name f-stack-2/db.c
Method dbBackup *backupDb(void) {

```
....
485.              sizeof(server.cluster->slots_keys_count));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=56
Status New

The size of the buffer used by slotToKeyFlush in ->, at line 1955 of f-stack-2/db.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that slotToKeyFlush passes to ->, at line 1955 of f-stack-2/db.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1960	1960
Object	->	->

Code Snippet
File Name f-stack-2/db.c
Method void slotToKeyFlush(int async) {

```
....
1960.             sizeof(server.cluster->slots_keys_count));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=57
Status	New

The size of the buffer used by SetRequiredAction1 in t_CcNodeInformation, at line 412 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SetRequiredAction1 passes to t_CcNodeInformation, at line 412 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	448	448
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error SetRequiredAction1(

```
....
448.                          memset(&ccNodeInfo, 0,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=58
Status	New

The size of the buffer used by ReleaseModifiedDataStructure in t_CcNodeInformation, at line 593 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ReleaseModifiedDataStructure passes to t_CcNodeInformation, at line 593 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	631	631
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error ReleaseModifiedDataStructure(

```
....
631.              memset(&ccNodeInfo, 0, sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=59
Status	New

The size of the buffer used by ReleaseModifiedDataStructure in t_CcNodeInformation, at line 593 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ReleaseModifiedDataStructure passes to t_CcNodeInformation, at line 593 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	649	649
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error ReleaseModifiedDataStructure(

```
....
649.                  memset(&ccNodeInfo, 0,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=60
Status	New

The size of the buffer used by BuildNewAd in t_FmPcdCcNode, at line 834 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BuildNewAd passes to t_FmPcdCcNode, at line 834 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	849	849
Object	t_FmPcdCcNode	t_FmPcdCcNode

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
849.      memset(p_FmPcdCcNodeTmp, 0, sizeof(t_FmPcdCcNode));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=61
Status	New

The size of the buffer used by DoDynamicChange in t_FmPcdCcNextEngineParams, at line 969 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DoDynamicChange passes to t_FmPcdCcNextEngineParams, at line 969 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	986	986
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error DoDynamicChange(

```
....
986.      memset(&nextEngineParams, 0,
sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=62
Status	New

The size of the buffer used by BuildNewNodeModifyNextEngine in t_CcNodeInformation, at line 3094 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BuildNewNodeModifyNextEngine passes to t_CcNodeInformation, at line 3094 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3193	3193
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3193.       memset(&ccNodeInfo, 0, sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=63
Status New

The size of the buffer used by BuildNewNodeModifyNextEngine in t_CcNodeInformation, at line 3094 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BuildNewNodeModifyNextEngine passes to t_CcNodeInformation, at line 3094 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3207	3207
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3207.       memset(&ccNodeInfo, 0, sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=64
Status New

The size of the buffer used by UpdateAdPtrOfNodesWhichPointsOnCrntMdfNode in t_CcNodeInformation, at line 3331 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that UpdateAdPtrOfNodesWhichPointsOnCrntMdfNode passes to t_CcNodeInformation, at line 3331 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3369	3369
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void UpdateAdPtrOfNodesWhichPointsOnCrntMdfNode(

```
....
3369.                       memset(&ccNodeInfo, 0,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=65
Status New

The size of the buffer used by UpdateAdPtrOfTreesWhichPointsOnCrntMdfNode in t_CcNodeInformation, at line 3384 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that UpdateAdPtrOfTreesWhichPointsOnCrntMdfNode passes to t_CcNodeInformation, at line 3384 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3414	3414
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static void UpdateAdPtrOfTreesWhichPointsOnCrntMdfNode(

```
....
3414.                       memset(&ccNodeInfo, 0,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=66
Status New

The size of the buffer used by ModifyNodeCommonPart in t_FmPcdModifyCcKeyAdditionalParams, at line 3429 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that ModifyNodeCommonPart passes to t_FmPcdModifyCcKeyAdditionalParams, at line 3429 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3510	3510
Object	t_FmPcdModifyCcKeyAdditionalParams	t_FmPcdModifyCcKeyAdditionalParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

```
....
3510.              sizeof(t_FmPcdModifyCcKeyAdditionalParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=67
Status New

The size of the buffer used by AllocStatsObjs in t_FmPcdStatsObj, at line 4227 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AllocStatsObjs passes to t_FmPcdStatsObj, at line 4227 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4248	4248
Object	t_FmPcdStatsObj	t_FmPcdStatsObj

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error AllocStatsObjs(t_FmPcdCcNode *p_CcNode)

```
....
4248.           memset(p_StatsObj, 0, sizeof(t_FmPcdStatsObj));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=68
Status New

The size of the buffer used by MatchTableGetKeyStatistics in t_FmPcdCcKeyStatistics, at line 4286 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that MatchTableGetKeyStatistics passes to t_FmPcdCcKeyStatistics, at line 4286 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4300	4300
Object	t_FmPcdCcKeyStatistics	t_FmPcdCcKeyStatistics

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableGetKeyStatistics(

```
....
4300.       memset(p_KeyStatistics, 0, sizeof(t_FmPcdCcKeyStatistics));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=69
Status	New

The size of the buffer used by MatchTableSet in t_CcNodeInformation, at line 4324 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that MatchTableSet passes to t_CcNodeInformation, at line 4324 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4839	4839
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4839.                   memset(&ccNodeInfo, 0,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=70
Status	New

The size of the buffer used by MatchTableSet in t_CcNodeInformation, at line 4324 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that MatchTableSet passes to t_CcNodeInformation, at line 4324 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4858	4858
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4858.                       memset(&ccNodeInfo, 0,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=71
Status New

The size of the buffer used by EnqueueNodeInfoToRelevantLst in t_CcNodeInformation, at line 4938 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EnqueueNodeInfoToRelevantLst passes to t_CcNodeInformation, at line 4938 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4949	4949
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method void EnqueueNodeInfoToRelevantLst(t_List *p_List, t_CcNodeInformation *p_CcInfo,

```
....
4949.          memset(p_CcInformation, 0, sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=72
Status New

The size of the buffer used by FmPcdCcTreeAddIPR in t_FmPcdCcNextEngineParams, at line 5046 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FmPcdCcTreeAddIPR passes to t_FmPcdCcNextEngineParams, at line 5046 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5062	5062
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5062.       memset(&nextEngineParams, 0,
sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=73
Status New

The size of the buffer used by FmPcdCcTreeAddIPR in t_NetEnvParams, at line 5046 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FmPcdCcTreeAddIPR passes to t_NetEnvParams, at line 5046 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5063	5063
Object	t_NetEnvParams	t_NetEnvParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5063.       memset(&netEnvParams, 0, sizeof(t_NetEnvParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=74
Status New

The size of the buffer used by FmPcdCcTreeAddCPR in t_FmPcdCcNextEngineParams, at line 5158 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FmPcdCcTreeAddCPR passes to t_FmPcdCcNextEngineParams, at line 5158 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5172	5172
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcTreeAddCPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5172.       memset(&nextEngineParams, 0,
sizeof(t_FmPcdCcNextEngineParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=75
Status New

The size of the buffer used by FmPcdCcTreeAddCPR in t_NetEnvParams, at line 5158 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FmPcdCcTreeAddCPR passes to t_NetEnvParams, at line 5158 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5173	5173
Object	t_NetEnvParams	t_NetEnvParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcTreeAddCPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5173.       memset(&netEnvParams, 0, sizeof(t_NetEnvParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=76
Status New

The size of the buffer used by FmPcdCcNodeTreeTryLock in t_CcNodeInformation, at line 5824 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FmPcdCcNodeTreeTryLock passes to t_CcNodeInformation, at line 5824 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5854	5854
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcNodeTreeTryLock(t_Handle h_FmPcd, t_Handle h_FmPcdCcNode,

```
....
5854.          memset(&nodeInfo, 0, sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=77
Status New

The size of the buffer used by FmPcdCcGetAdTablesThatPointOnReplicGroup in t_CcNodeInformation, at line 5953 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FmPcdCcGetAdTablesThatPointOnReplicGroup passes to t_CcNodeInformation, at line 5953 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5978	5978
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method void FmPcdCcGetAdTablesThatPointOnReplicGroup(t_Handle h_Node,

```
....
5978.              memset(&ccNodeInfo, 0, sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=78
Status New

The size of the buffer used by FM_PCD_CcRootBuild in t_FmPcdCcTree, at line 5994 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_CcRootBuild passes to t_FmPcdCcTree, at line 5994 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6026	6026
Object	t_FmPcdCcTree	t_FmPcdCcTree

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6026.       memset(p_FmPcdCcTree, 0, sizeof(t_FmPcdCcTree));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=79
Status New

The size of the buffer used by FM_PCD_CcRootBuild in t_CcNodeInformation, at line 5994 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_CcRootBuild passes to t_CcNodeInformation, at line 5994 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6217	6217
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6217.                   memset(&ccNodeInfo, 0,
sizeof(t_CcNodeInformation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=80
Status New

The size of the buffer used by FM_PCD_MatchTableSet in t_FmPcdCcNode, at line 6382 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_MatchTableSet passes to t_FmPcdCcNode, at line 6382 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6397	6397
Object	t_FmPcdCcNode	t_FmPcdCcNode

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_MatchTableSet(t_Handle h_FmPcd,

```
....
6397.       memset(p_CcNode, 0, sizeof(t_FmPcdCcNode));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=81
Status New

The size of the buffer used by FM_PCD_HashTableSet in t_FmPcdCcNodeParams, at line 7113 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_HashTableSet passes to t_FmPcdCcNodeParams, at line 7113 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	7163	7163
Object	t_FmPcdCcNodeParams	t_FmPcdCcNodeParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_HashTableSet(t_Handle h_FmPcd, t_FmPcdHashTableParams *p_Param)

```
....
7163.       memset(p_ExactMatchCcNodeParam, 0,
sizeof(t_FmPcdCcNodeParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=82
Status New

The size of the buffer used by FM_PCD_HashTableSet in t_FmPcdCcNodeParams, at line 7113 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_HashTableSet passes to t_FmPcdCcNodeParams, at line 7113 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	7173	7173
Object	t_FmPcdCcNodeParams	t_FmPcdCcNodeParams

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_HashTableSet(t_Handle h_FmPcd, t_FmPcdHashTableParams *p_Param)

```
....
7173.       memset(p_IndxHashCcNodeParam, 0,
sizeof(t_FmPcdCcNodeParams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=83
Status New

The size of the buffer used by FM_PCD_HashTableSet in t_FmPcdCcNode, at line 7113 of f-stack-2/fm_cc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that FM_PCD_HashTableSet passes to t_FmPcdCcNode, at line 7113 of f-stack-2/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	7243	7243
Object	t_FmPcdCcNode	t_FmPcdCcNode

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_HashTableSet(t_Handle h_FmPcd, t_FmPcdHashTableParams *p_Param)

```
....
7243.           memset(p_CcNode, 0, sizeof(t_FmPcdCcNode));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=300

	36&pathid=84
Status	New

The size of the buffer used by initSentinel in Namespace913672341, at line 509 of f-stack-2/sentinel.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that initSentinel passes to Namespace913672341, at line 509 of f-stack-2/sentinel.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	548	548
Object	Namespace913672341	Namespace913672341

Code Snippet
File Name f-stack-2/sentinel.c
Method void initSentinel(void) {

```
....
548.      memset(sentinel.myid,0,sizeof(sentinel.myid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=85
Status	New

The size of the buffer used by add_bbdev_dev in rte_fpga_lte_fec_conf, at line 611 of f-stack-2/test_bbdev_perf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that add_bbdev_dev passes to rte_fpga_lte_fec_conf, at line 611 of f-stack-2/test_bbdev_perf.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	634	634
Object	rte_fpga_lte_fec_conf	rte_fpga_lte_fec_conf

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method add_bbdev_dev(uint8_t dev_id, struct rte_bbdev_info *info,

```
....
634.              memset(&conf, 0, sizeof(struct
rte_fpga_lte_fec_conf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=300

	36&pathid=86
Status	New

The size of the buffer used by add_bbdev_dev in rte_fpga_5gnr_fec_conf, at line 611 of f-stack-2/test_bbdev_perf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that add_bbdev_dev passes to rte_fpga_5gnr_fec_conf, at line 611 of f-stack-2/test_bbdev_perf.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	678	678
Object	rte_fpga_5gnr_fec_conf	rte_fpga_5gnr_fec_conf

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method add_bbdev_dev(uint8_t dev_id, struct rte_bbdev_info *info,

```
....
678.              memset(&conf, 0, sizeof(struct
rte_fpga_5gnr_fec_conf));
```

Use After Free

Query Path:
CPP\Cx\CPP Medium Threat\Use After Free Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Use After Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=403
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4279
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4279.           ngx_close_connection(u->peer.connection);
```

Use After Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=404
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4279
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4279.           ngx_close_connection(u->peer.connection);
```

Use After Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=405
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4276
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4276.              ngx_destroy_pool(u->peer.connection->pool);
```

Use After Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=406
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4276
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4276.              ngx_destroy_pool(u->peer.connection->pool);
```

Use After Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=407
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4275
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4275.           if (u->peer.connection->pool) {
```

Use After Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=408
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4275
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4275.           if (u->peer.connection->pool) {
```

Use After Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=409
Status	New

The pointer connection at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4271
Object	Address	connection

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4271.              (void) ngx_ssl_shutdown(u->peer.connection);
```

Use After Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=410
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4271
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4271.              (void) ngx_ssl_shutdown(u->peer.connection);
```

Use After Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=411
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4271
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4271.              (void) ngx_ssl_shutdown(u->peer.connection);
```

Use After Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=412
Status	New

The pointer connection at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4267
Object	Address	connection

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4267.          if (u->peer.connection->ssl) {
```

Use After Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=413
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4267
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4267.           if (u->peer.connection->ssl) {
```

Use After Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=414
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4267
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4267.           if (u->peer.connection->ssl) {
```

Use After Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=415
Status	New

The pointer connection at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4264
Object	Address	connection

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4264.                              u->peer.connection->fd);
```

Use After Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=416
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4264
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4264.                              u->peer.connection->fd);
```

Use After Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=417
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4264
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4264.                              u->peer.connection->fd);
```

Use After Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=418
Status	New

The pointer connection at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4261
Object	Address	connection

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4261.      if (u->peer.connection) {
```

Use After Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=419
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4261
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4261.      if (u->peer.connection) {
```

Use After Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=420
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4261
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4261.      if (u->peer.connection) {
```

Use After Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=421
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4222
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4222.      if (u->peer.tries == 0
```

Use After Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=422
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4222
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4222.      if (u->peer.tries == 0
```

Use After Free\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=423
Status	New

The pointer start_time at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4225
Object	Address	start_time

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4225.           || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

Use After Free\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=424
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4225
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4225.           || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

Use After Free\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=425
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4225
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4225.           || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

Use After Free\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=426
Status	New

The pointer tries at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4167
Object	Address	tries

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4167.           u->peer.tries++;
```

Use After Free\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=427
Status	New

The pointer cached at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4165
Object	Address	cached

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4165.      if (u->peer.cached && ft_type == NGX_HTTP_UPSTREAM_FT_ERROR)
{
```

Use After Free\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=428
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4165
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.          u->peer.free(&u->peer, u->peer.data, state);
....
4165.      if (u->peer.cached && ft_type == NGX_HTTP_UPSTREAM_FT_ERROR)
{
```

Use After Free\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=429
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4132 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4156	4165
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_next(ngx_http_request_t *r, ngx_http_upstream_t *u,

```
....
4156.           u->peer.free(&u->peer, u->peer.data, state);
....
4165.       if (u->peer.cached && ft_type == NGX_HTTP_UPSTREAM_FT_ERROR)
{
```

Use After Free\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=430
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4371
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.           u->peer.free(&u->peer, u->peer.data, 0);
....
4371.           ngx_close_connection(u->peer.connection);
```

Use After Free\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=431
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4371
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4371.          ngx_close_connection(u->peer.connection);
```

Use After Free\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=432
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4368
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4368.              ngx_destroy_pool(u->peer.connection->pool);
```

Use After Free\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=433
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4368
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4368.              ngx_destroy_pool(u->peer.connection->pool);
```

Use After Free\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=434
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4367
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4367.          if (u->peer.connection->pool) {
```

Use After Free\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=435
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4367
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4367.          if (u->peer.connection->pool) {
```

Use After Free\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=436
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4365
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4365.                          u->peer.connection->fd);
```

Use After Free\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=437
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4365
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4365.                              u->peer.connection->fd);
```

Use After Free\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=438
Status	New

The pointer connection at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4359
Object	Address	connection

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4359.              (void) ngx_ssl_shutdown(u->peer.connection);
```

Use After Free\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=439
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4359
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4359.              (void) ngx_ssl_shutdown(u->peer.connection);
```

Use After Free\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=440
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4359
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4359.              (void) ngx_ssl_shutdown(u->peer.connection);
```

Use After Free\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=441
Status	New

The pointer connection at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4349
Object	Address	connection

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.           u->peer.free(&u->peer, u->peer.data, 0);
....
4349.           if (u->peer.connection->ssl) {
```

Use After Free\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=442
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4349
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.           u->peer.free(&u->peer, u->peer.data, 0);
....
4349.           if (u->peer.connection->ssl) {
```

Use After Free\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=443
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4349
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4349.          if (u->peer.connection->ssl) {
```

Use After Free\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=444
Status	New

The pointer connection at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4343
Object	Address	connection

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4343.      if (u->peer.connection) {
```

Use After Free\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=445
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4343
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4343.      if (u->peer.connection) {
```

Use After Free\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=446
Status	New

The pointer peer at f-stack-2/ngx_http_upstream.c in line 4300 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4339	4343
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_finalize_request(ngx_http_request_t *r,

```
....
4339.          u->peer.free(&u->peer, u->peer.data, 0);
....
4343.      if (u->peer.connection) {
```

Use After Free\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=447
Status	New

The pointer tries at f-stack-2/ngx_stream_proxy_module.c in line 1790 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_stream_proxy_module.c	f-stack-2/ngx_stream_proxy_module.c
Line	1815	1823
Object	Address	tries

Code Snippet
File Name f-stack-2/ngx_stream_proxy_module.c
Method ngx_stream_proxy_next_upstream(ngx_stream_session_t *s)

```
....
1815.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1823.      if (u->peer.tries == 0
```

Use After Free\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=448
Status	New

The pointer peer at f-stack-2/ngx_stream_proxy_module.c in line 1790 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_stream_proxy_module.c	f-stack-2/ngx_stream_proxy_module.c
Line	1815	1823
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_stream_proxy_module.c
Method ngx_stream_proxy_next_upstream(ngx_stream_session_t *s)

```
....
1815.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1823.      if (u->peer.tries == 0
```

Use After Free\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=449
Status	New

The pointer peer at f-stack-2/ngx_stream_proxy_module.c in line 1790 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_stream_proxy_module.c	f-stack-2/ngx_stream_proxy_module.c
Line	1815	1823
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_stream_proxy_module.c
Method ngx_stream_proxy_next_upstream(ngx_stream_session_t *s)

```
....
1815.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1823.      if (u->peer.tries == 0
```

Use After Free\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=450
Status	New

The pointer start_time at f-stack-2/ngx_stream_proxy_module.c in line 1790 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_stream_proxy_module.c	f-stack-2/ngx_stream_proxy_module.c
Line	1815	1825
Object	Address	start_time

Code Snippet
File Name f-stack-2/ngx_stream_proxy_module.c
Method ngx_stream_proxy_next_upstream(ngx_stream_session_t *s)

```
....
1815.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1825.          || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

Use After Free\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=451
Status	New

The pointer peer at f-stack-2/ngx_stream_proxy_module.c in line 1790 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_stream_proxy_module.c	f-stack-2/ngx_stream_proxy_module.c
Line	1815	1825
Object	Address	peer

Code Snippet
File Name f-stack-2/ngx_stream_proxy_module.c
Method ngx_stream_proxy_next_upstream(ngx_stream_session_t *s)

```
....
1815.           u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1825.           || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

Use After Free\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=452
Status	New

The pointer peer at f-stack-2/ngx_stream_proxy_module.c in line 1790 is being used after it has been freed.

	Source	Destination
File	f-stack-2/ngx_stream_proxy_module.c	f-stack-2/ngx_stream_proxy_module.c
Line	1815	1825
Object	data	peer

Code Snippet
File Name f-stack-2/ngx_stream_proxy_module.c
Method ngx_stream_proxy_next_upstream(ngx_stream_session_t *s)

```
....
1815.           u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1825.           || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=1
Status	New

The application performs an illegal operation in print_dec_bler, in f-stack-2/test_bbdev_perf.c. In line 3685, the program attempts to divide by used_cores, 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 used_cores in print_dec_bler of f-stack-2/test_bbdev_perf.c, at line 3685.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c

Line	3702	3702
Object	used_cores	used_cores

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method print_dec_bler(struct thread_params *t_params, unsigned int used_cores)

```
....
3702.       total_bler /= used_cores;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=2
Status	New

The application performs an illegal operation in print_dec_bler, in f-stack-2/test_bbdev_perf.c. In line 3685, the program attempts to divide by used_cores, 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 used_cores in print_dec_bler of f-stack-2/test_bbdev_perf.c, at line 3685.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	3703	3703
Object	used_cores	used_cores

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method print_dec_bler(struct thread_params *t_params, unsigned int used_cores)

```
....
3703.       total_iter /= used_cores;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=3
Status	New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by g_fxp, 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 g_fxp in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination

File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1554	1554
Object	g_fxp	g_fxp

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1554.          x_est[bin] = ((y_est[bin] * 1 << scale_factor) + g_fxp) /
g_fxp;
```

Divide By Zero\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=4
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by g_fxp, 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 g_fxp in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1565	1565
Object	g_fxp	g_fxp

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1565.              x_est[bin] - ((1 << scale_factor) * y_est[bin] +
g_fxp) / g_fxp;
```

Divide By Zero\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=5
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1638	1638
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1638.           x_tilde[bin] = x_tilde[bin] / (1 << q_x);
```

Divide By Zero\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=6
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1639	1639
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1639.           b1_tmp[bin] = b1_tmp[bin] / (1 << q_b1);
```

Divide By Zero\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=7
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1640	1640
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1640.           b2_tmp[bin] = b2_tmp[bin] / (1 << q_b2);
```

Divide By Zero\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=8
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by scale_b, 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 scale_b in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1665	1665
Object	scale_b	scale_b

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1665.       alpha = (alpha_raw << 10) / scale_b;
```

Divide By Zero\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=9
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by scale_b, 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 scale_b in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1666	1666
Object	scale_b	scale_b

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1666.       beta = (beta_raw << 10) / scale_b;
```

Divide By Zero\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=10
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by g_fxp, 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 g_fxp in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1691	1691
Object	g_fxp	g_fxp

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1691.           pa_in[idx] = y5 + y3 + (256 * tmp) / g_fxp;
```

Divide By Zero\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=11
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by scale_b, 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 scale_b in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1740	1740
Object	scale_b	scale_b

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1740.       alpha = (alpha_raw << 10) / scale_b;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=12
Status	New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by scale_b, 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 scale_b in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1741	1741
Object	scale_b	scale_b

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1741.       beta = (beta_raw << 10) / scale_b;
```

Divide By Zero\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=13
Status	New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1756	1756
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1756.                   (1 << order1_5x)) / (1 << order1_5x);
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=14
Status	New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1759	1759
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1759.                       (1 << order1_5x)) / (1 << order1_5x));
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=15
Status	New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1762	1762
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1762.           y5 = (y5 * tmp) / (1 << order1_5x);
```

Divide By Zero\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=16
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1763	1763
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1763.           y5 = (y5 * tmp) / (1 << order1_5x);
```

Divide By Zero\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=17
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1764	1764
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1764.           y5 = (y5 * tmp) / (1 << order1_5x);
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=18
Status	New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1765	1765
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1765.           y5 = (y5 * tmp) / (1 << order1_5x);
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=19
Status	New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1770	1770
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1770.               y3 = (alpha * tmp - (1 << order2_3x)) / (1 <<
order2_3x);
```

Divide By Zero\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=20
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1772	1772
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1772.               y3 = (alpha * tmp + (1 << order2_3x)) / (1 <<
order2_3x);
```

Divide By Zero\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=21
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1775	1775
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1775.           y3 = (y3 * tmp) / (1 << order2_3x);
```

Divide By Zero\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=22
Status New

The application performs an illegal operation in create_pa_curve, in f-stack-2/ar9300_paprd.c. In line 1385, the program attempts to divide by AssignExpr, 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 AssignExpr in create_pa_curve of f-stack-2/ar9300_paprd.c, at line 1385.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1776	1776
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1776.           y3 = (y3 * tmp) / (1 << order2_3x);
```

Divide By Zero\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=23
Status New

The application performs an illegal operation in ngx_resolver_report_srv, in f-stack-2/ngx_resolver.c. In line 4245, the program attempts to divide by nw, 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 nw in ngx_resolver_report_srv of f-stack-2/ngx_resolver.c, at line 4245.

	Source	Destination
File	f-stack-2/ngx_resolver.c	f-stack-2/ngx_resolver.c
Line	4311	4311
Object	nw	nw

Code Snippet
File Name f-stack-2/ngx_resolver.c
Method ngx_resolver_report_srv(ngx_resolver_t *r, ngx_resolver_ctx_t *ctx)

```
....
4311.           w = ngx_random() % nw;
```

Divide By Zero\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=24
Status	New

The application performs an illegal operation in validation_latency_test, in f-stack-2/test_bbdev_perf.c. In line 4265, the program attempts to divide by iter, 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 iter in validation_latency_test of f-stack-2/test_bbdev_perf.c, at line 4265.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	4328	4328
Object	iter	iter

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method validation_latency_test(struct active_device *ad,

```
....
4328.                       (double)total_time / (double)iter,
```

Divide By Zero\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=25
Status	New

The application performs an illegal operation in validation_latency_test, in f-stack-2/test_bbdev_perf.c. In line 4265, the program attempts to divide by iter, 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 iter in validation_latency_test of f-stack-2/test_bbdev_perf.c, at line 4265.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	4329	4329
Object	iter	iter

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method validation_latency_test(struct active_device *ad,

```
....
4329.                    (double)(total_time * 1000000) / (double)iter /
```

Divide By Zero\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=26
Status New

The application performs an illegal operation in d2string, in f-stack-2/util.c. In line 543, the program attempts to divide by value, 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 value in d2string of f-stack-2/util.c, at line 543.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	553	553
Object	value	value

Code Snippet
File Name f-stack-2/util.c
Method int d2string(char *buf, size_t len, double value) {

```
....
553.          if (1.0/value < 0)
```

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

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=163
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2417 of f-stack-2/icmp6.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2594	2594
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2594.             len = maxlen - (p - (u_char *)ip6);
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=164
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of f-stack-2/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/sort.c	f-stack-2/sort.c
Line	346	346
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/sort.c
Method void sortCommand(client *c) {

```
....
346.          vectorlen = end-start+1;
```

Integer Overflow\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=165
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of f-stack-2/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/sort.c	f-stack-2/sort.c
Line	510	510
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/sort.c
Method void sortCommand(client *c) {

```
....
510.        outputlen = getop ? getop*(end-start+1) : end-start+1;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=166
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of f-stack-2/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/sort.c	f-stack-2/sort.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/sort.c
Method void sortCommand(client *c) {

```
....
516.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=167
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 192 of f-stack-2/sort.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/sort.c	f-stack-2/sort.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/sort.c
Method void sortCommand(client *c) {

```
....
544.            for (j = start; j <= end; j++) {
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=168
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of f-stack-2/subr_scanf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/subr_scanf.c	f-stack-2/subr_scanf.c
Line	328	328
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/subr_scanf.c
Method vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
328.                                        inr -= width;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=169
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of f-stack-2/subr_scanf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	f-stack-2/subr_scanf.c	f-stack-2/subr_scanf.c
Line	336	336
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/subr_scanf.c
Method vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
336.                            inr -= width;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=170
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of f-stack-2/subr_scanf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/subr_scanf.c	f-stack-2/subr_scanf.c
Line	338	338
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/subr_scanf.c
Method vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
338.                            nread += width;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=171
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of f-stack-2/subr_scanf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/subr_scanf.c	f-stack-2/subr_scanf.c
Line	333	333
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	f-stack-2/subr_scanf.c
Method	vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
333.                           nread += sum;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=172
Status	New

A variable of a larger data type, cmd_items, is being assigned to a smaller data type, in 993 of f-stack-2/aof.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1003	1003
Object	cmd_items	cmd_items

Code Snippet	
File Name	f-stack-2/aof.c
Method	int rewriteListObject(rio *r, robj *key, robj *o) {

```
....
1003.                   int cmd_items = (items >
AOF_REWRITE_ITEMS_PER_CMD) ?
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=173
Status	New

A variable of a larger data type, cmd_items, is being assigned to a smaller data type, in 1037 of f-stack-2/aof.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1046	1046
Object	cmd_items	cmd_items

Code Snippet	
File Name	f-stack-2/aof.c
Method	int rewriteSetObject(rio *r, robj *key, robj *o) {

```
....
1046.                   int cmd_items = (items >
AOF_REWRITE_ITEMS_PER_CMD) ?
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=174
Status	New

A variable of a larger data type, cmd_items, is being assigned to a smaller data type, in 1037 of f-stack-2/aof.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1067	1067
Object	cmd_items	cmd_items

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteSetObject(rio *r, robj *key, robj *o) {

```
....
1067.                   int cmd_items = (items >
AOF_REWRITE_ITEMS_PER_CMD) ?
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=175
Status	New

A variable of a larger data type, cmd_items, is being assigned to a smaller data type, in 1094 of f-stack-2/aof.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1115	1115
Object	cmd_items	cmd_items

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteSortedSetObject(rio *r, robj *key, robj *o) {

```
....
1115.                   int cmd_items = (items >
AOF_REWRITE_ITEMS_PER_CMD) ?
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=176
Status	New

A variable of a larger data type, cmd_items, is being assigned to a smaller data type, in 1094 of f-stack-2/aof.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1145	1145
Object	cmd_items	cmd_items

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteSortedSetObject(rio *r, robj *key, robj *o) {

```
....
1145.                   int cmd_items = (items >
AOF_REWRITE_ITEMS_PER_CMD) ?
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=177
Status	New

A variable of a larger data type, cmd_items, is being assigned to a smaller data type, in 1200 of f-stack-2/aof.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1207	1207
Object	cmd_items	cmd_items

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteHashObject(rio *r, robj *key, robj *o) {

```
....
1207.              int cmd_items = (items > AOF_REWRITE_ITEMS_PER_CMD) ?
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=178
Status	New

A variable of a larger data type, copylen, is being assigned to a smaller data type, in 647 of f-stack-2/util.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	678	678
Object	copylen	copylen

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
678.          unsigned int copylen =
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=453
Status	New

The variable declared in ifp at f-stack-2/icmp6.c in line 1653 is not initialized when it is used by ifp at f-stack-2/icmp6.c in line 1653.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1656	1732
Object	ifp	ifp

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_addrs(struct icmp6_nodeinfo *ni6, struct mbuf *m, struct ifnet **ifpp,

```
....
1656.        struct ifnet *ifp;
....
1732.                    *ifpp = ifp;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=454
Status	New

The variable declared in nip6 at f-stack-2/icmp6.c in line 259 is not initialized when it is used by ip6_dst at f-stack-2/icmp6.c in line 259.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	261	371
Object	nip6	ip6_dst

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_error(struct mbuf *m, int type, int code, int param)

```
....
261.        struct ip6_hdr *oip6, *nip6;
....
371.        nip6->ip6_dst  = oip6->ip6_dst;
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=455
Status	New

The variable declared in nip6 at f-stack-2/icmp6.c in line 259 is not initialized when it is used by ip6_src at f-stack-2/icmp6.c in line 259.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	261	370
Object	nip6	ip6_src

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_error(struct mbuf *m, int type, int code, int param)

```
....
261.        struct ip6_hdr *oip6, *nip6;
....
370.        nip6->ip6_src  = oip6->ip6_src;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=456
Status	New

The variable declared in nip6 at f-stack-2/icmp6.c in line 259 is not initialized when it is used by nip6 at f-stack-2/icmp6.c in line 259.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	261	376
Object	nip6	nip6

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_error(struct mbuf *m, int type, int code, int param)

```
....
261.        struct ip6_hdr *oip6, *nip6;
....
376.        icmp6 = (struct icmp6_hdr *)(nip6 + 1);
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=457
Status	New

The variable declared in ifa at f-stack-2/icmp6.c in line 1653 is not initialized when it is used by ifa at f-stack-2/icmp6.c in line 1653.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1658	1684
Object	ifa	ifa

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_addrs(struct icmp6_nodeinfo *ni6, struct mbuf *m, struct ifnet **ifpp,

```
....
1658.       struct ifaddr *ifa;
....
1684.                   ifa6 = (struct in6_ifaddr *)ifa;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=458
Status	New

The variable declared in ifa at f-stack-2/icmp6.c in line 1653 is not initialized when it is used by ifa_addr at f-stack-2/icmp6.c in line 1653.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1658	1682
Object	ifa	ifa_addr

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_addrs(struct icmp6_nodeinfo *ni6, struct mbuf *m, struct ifnet **ifpp,

```
....
1658.       struct ifaddr *ifa;
....
1682.                   if (ifa->ifa_addr->sa_family != AF_INET6)
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=459
Status	New

The variable declared in ifa at f-stack-2/icmp6.c in line 1743 is not initialized when it is used by ifa at f-stack-2/icmp6.c in line 1743.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1748	1767
Object	ifa	ifa

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1748.       struct ifaddr *ifa;
....
1767.                   ifa6 = (struct in6_ifaddr *)ifa;
```

Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=460
Status	New

The variable declared in ifa at f-stack-2/icmp6.c in line 1743 is not initialized when it is used by ifa_addr at f-stack-2/icmp6.c in line 1743.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1748	1765
Object	ifa	ifa_addr

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1748.       struct ifaddr *ifa;
....
1765.                   if (ifa->ifa_addr->sa_family != AF_INET6)
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=461
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1681	1686
Object	byte	byte

Code Snippet
File Name f-stack-2/aof.c
Method void aofChildPipeReadable(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
1681.       char byte;
....
1686.       if (read(fd,&byte,1) == 1 && byte == '!') {
```

Use of Uninitialized Variable\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=462
Status New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	452	464
Object	llbits	llbits

Code Snippet
File Name f-stack-2/bitops.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
464.          llbits < 1 ||
```

Use of Uninitialized Variable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=463
Status New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	452	465

Object	llbits	llbits

Code Snippet
File Name f-stack-2/bitops.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
465.           (*sign == 1 && llbits > 64) ||
```

Use of Uninitialized Variable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=464
Status New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	452	466
Object	llbits	llbits

Code Snippet
File Name f-stack-2/bitops.c
Method int getBitfieldTypeFromArgument(client *c, robj *o, int *sign, int *bits) {

```
....
452.      long long llbits;
....
466.           (*sign == 0 && llbits > 63))
```

Use of Uninitialized Variable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=465
Status New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	3159	3173
Object	numval	numval

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelConfigSetCommand(client *c) {

```
....
3159.       long long numval;
....
3173.               numval < 0 || numval > 65535)
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=466
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	3159	3173
Object	numval	numval

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelConfigSetCommand(client *c) {

```
....
3159.       long long numval;
....
3173.               numval < 0 || numval > 65535)
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=647
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of f-stack-2/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of f-stack-2/util.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c

Line	659	693
Object	seed	kxor

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=648
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of f-stack-2/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of f-stack-2/util.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	659	693
Object	seed	sizeof

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
693.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=649
Status	New

The size of the buffer used by getRandomBytes in kxor, at line 647 of f-stack-2/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of f-stack-2/util.c, to overwrite the target buffer.

	Source	Destination

File	f-stack-2/util.c	f-stack-2/util.c
Line	659	682
Object	seed	kxor

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=650
Status	New

The size of the buffer used by getRandomBytes in sizeof, at line 647 of f-stack-2/util.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getRandomBytes passes to seed, at line 647 of f-stack-2/util.c, to overwrite the target buffer.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	659	682
Object	seed	sizeof

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
....
682.          memcpy(kxor,seed,sizeof(kxor));
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

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

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=161
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1986 of f-stack-2/db.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1991	1991
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/db.c
Method unsigned int delKeysInSlot(unsigned int hashslot) {

```
....
1991.       indexed[0] = (hashslot >> 8) & 0xff;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=162
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1986 of f-stack-2/db.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1992	1992
Object	AssignExpr	AssignExpr

Code Snippet
File Name f-stack-2/db.c
Method unsigned int delKeysInSlot(unsigned int hashslot) {

```
....
1992.       indexed[1] = hashslot & 0xff;
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=399
Status	New

Method tlsPasswordCallback at line 186 of f-stack-2/tls.c defines pass_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass_len, this variable is never cleared from memory.

	Source	Destination
File	f-stack-2/tls.c	f-stack-2/tls.c
Line	190	190
Object	pass_len	pass_len

Code Snippet
File Name f-stack-2/tls.c
Method static int tlsPasswordCallback(char *buf, int size, int rwflag, void *u) {

```
....
190.      size_t pass_len;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=400
Status	New

Method tlsPasswordCallback at line 186 of f-stack-2/tls.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	f-stack-2/tls.c	f-stack-2/tls.c
Line	189	189
Object	pass	pass

Code Snippet
File Name f-stack-2/tls.c
Method static int tlsPasswordCallback(char *buf, int size, int rwflag, void *u) {

```
....
189.      const char *pass = u;
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=401
Status	New

	Source	Destination
File	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	1192	1192
Object	ts	ts

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method build_blockcipher_test_suite(enum blockcipher_test_type test_type)

```
....
1192.        ts = calloc(1, sizeof(struct unit_test_suite) +
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=402
Status	New

	Source	Destination
File	f-stack-2/vhost.c	f-stack-2/vhost.c
Line	927	927
Object	m	m

Code Snippet
File Name f-stack-2/vhost.c
Method rte_vhost_get_mem_table(int vid, struct rte_vhost_memory **mem)

```
....
927.        m = malloc(sizeof(struct rte_vhost_memory) + size);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=160
Status	New

The function size in f-stack-2/vhost.c at line 916 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	f-stack-2/vhost.c	f-stack-2/vhost.c
Line	927	927
Object	size	size

Code Snippet
File Name f-stack-2/vhost.c
Method rte_vhost_get_mem_table(int vid, struct rte_vhost_memory **mem)

```
....
927.        m = malloc(sizeof(struct rte_vhost_memory) + size);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=780
Status	New

The variable declared in null at f-stack-2/db.c in line 1028 is not initialized when it is used by type at f-stack-2/db.c in line 837.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1031	849
Object	null	type

Code Snippet
File Name f-stack-2/db.c
Method void scanCommand(client *c) {

```
....
1031.       scanGenericCommand(c,NULL,cursor);
```

File Name f-stack-2/db.c

Method void scanGenericCommand(client *c, robj *o, unsigned long cursor) {

```
....
849.       serverAssert(o == NULL || o->type == OBJ_SET || o->type ==
OBJ_HASH ||
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=781
Status	New

The variable declared in null at f-stack-2/db.c in line 1028 is not initialized when it is used by type at f-stack-2/db.c in line 837.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1031	849
Object	null	type

Code Snippet
File Name f-stack-2/db.c
Method void scanCommand(client *c) {

```
....
1031.       scanGenericCommand(c,NULL,cursor);
```

File Name f-stack-2/db.c

Method void scanGenericCommand(client *c, robj *o, unsigned long cursor) {

```
....
849.       serverAssert(o == NULL || o->type == OBJ_SET || o->type ==
OBJ_HASH ||
```

NULL Pointer Dereference\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=782
Status	New

The variable declared in null at f-stack-2/db.c in line 1028 is not initialized when it is used by type at f-stack-2/db.c in line 837.

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1031	850
Object	null	type

Code Snippet

File Name f-stack-2/db.c

Method void scanCommand(client *c) {

```
....
1031.       scanGenericCommand(c,NULL,cursor);
```

File Name f-stack-2/db.c

Method void scanGenericCommand(client *c, robj *o, unsigned long cursor) {

```
....
850.                    o->type == OBJ_ZSET);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=783
Status	New

The variable declared in null at f-stack-2/dsl_destroy.c in line 826 is not initialized when it is used by dd_myname at f-stack-2/dsl_destroy.c in line 826.

	Source	Destination
File	f-stack-2/dsl_destroy.c	f-stack-2/dsl_destroy.c
Line	835	867
Object	null	dd_myname

Code Snippet

File Name f-stack-2/dsl_destroy.c

Method dsl_dir_destroy_sync(uint64_t ddobj, dmu_tx_t *tx)

```
....
835.        VERIFY0(dsl_dir_hold_obj(dp, ddobj, NULL, FTAG, &dd));
....
867.            dd->dd_myname, tx));
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=784
Status	New

The variable declared in null at f-stack-2/dsl_destroy.c in line 826 is not initialized when it is used by dd_parent at f-stack-2/dsl_destroy.c in line 826.

	Source	Destination
File	f-stack-2/dsl_destroy.c	f-stack-2/dsl_destroy.c
Line	835	866
Object	null	dd_parent

Code Snippet
File Name f-stack-2/dsl_destroy.c
Method dsl_dir_destroy_sync(uint64_t ddobj, dmu_tx_t *tx)

```
....
835.        VERIFY0(dsl_dir_hold_obj(dp, ddobj, NULL, FTAG, &dd));
....
866.            dsl_dir_phys(dd->dd_parent)->dd_child_dir_zapobj,
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=785
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by xb_bufp at f-stack-2/enc_cbor.c in line 167.

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	248	182
Object	null	xb_bufp

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
```

File Name f-stack-2/enc_cbor.c

Method cbor_append (xo_handle_t *xop, cbor_private_t *cbor, xo_buffer_t *xbp,

```
....
182.                    xbp->xb_curp - xbp->xb_bufp - offset, "",
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=786
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by Pointer at f-stack-2/enc_cbor.c in line 167.

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	248	175
Object	null	Pointer

Code Snippet

File Name f-stack-2/enc_cbor.c

Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
```

File Name f-stack-2/enc_cbor.c

Method cbor_append (xo_handle_t *xop, cbor_private_t *cbor, xo_buffer_t *xbp,

```
....
175.      *xbp->xb_curp = major;
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=787
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by xb_bufp at f-stack-2/enc_cbor.c in line 204.

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	248	237
Object	null	xb_bufp

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
```

File Name f-stack-2/enc_cbor.c

Method cbor_content (xo_handle_t *xop, cbor_private_t *cbor, xo_buffer_t *xbp,

```
....
237.                  xbp->xb_curp - xbp->xb_bufp - offset, "",
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=788
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by xb_curp at f-stack-2/enc_cbor.c in line 204.

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	248	237
Object	null	xb_curp

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
```

File Name f-stack-2/enc_cbor.c

Method cbor_content (xo_handle_t *xop, cbor_private_t *cbor, xo_buffer_t *xbp,

```
....
237.                    xbp->xb_curp - xbp->xb_bufp - offset, "",
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=789
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by Pointer at f-stack-2/enc_cbor.c in line 204.

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	248	228
Object	null	Pointer

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
```

File Name f-stack-2/enc_cbor.c

Method cbor_content (xo_handle_t *xop, cbor_private_t *cbor, xo_buffer_t *xbp,

```
....
228.            *xbp->xb_curp = negative ? CBOR_NEGATIVE :
CBOR_UNSIGNED;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=790
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by xb_curp at f-stack-2/enc_cbor.c in line 244.

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c

Line	248	336
Object	null	xb_curp

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
....
336.                    xbp->xb_bufp, xbp->xb_curp - xbp->xb_bufp,
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=791
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by xb_bufp at f-stack-2/enc_cbor.c in line 244.

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	248	336
Object	null	xb_bufp

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
....
336.                    xbp->xb_bufp, xbp->xb_curp - xbp->xb_bufp,
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=792
Status	New

The variable declared in null at f-stack-2/enc_cbor.c in line 244 is not initialized when it is used by xb_bufp at f-stack-2/enc_cbor.c in line 244.

	Source	Destination

File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	248	336
Object	null	xb_bufp

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_handler (XO_ENCODER_HANDLER_ARGS)

```
....
248.      xo_buffer_t *xbp = cbor ? &cbor->c_data : NULL;
....
336.                    xbp->xb_bufp, xbp->xb_curp - xbp->xb_bufp,
```

NULL Pointer Dereference\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=793
Status New

The variable declared in null at f-stack-2/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	890	255
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
890.                    h_Ad, NULL, p_CcNode->h_FmPcd, p_FmPcdCcNodeTmp,
```

File Name f-stack-2/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=300

	36&pathid=794
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	881	255
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
881.           FillAdOfTypeContLookup(h_Ad, NULL, p_CcNode->h_FmPcd,
p_FmPcdCcNodeTmp,
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.       if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=795
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 377 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	403	255
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error AllocAndFillAdForContLookupManip(t_Handle h_CcNode)

```
....
403.          FillAdOfTypeContLookup(p_CcNode->h_Ad, NULL, p_CcNode-
>h_FmPcd,
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=796
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 3094 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3239	255
Object	null	h_StatsFLRs

Code Snippet

File Name f-stack-2/fm_cc.c

Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3239.          NextStepAd(p_Ad, NULL, p_CcNextEngineParams, h_FmPcd);
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=797
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 2566 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2686	255
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2686.                   NextStepAd(p_AdTableNewTmp, NULL,
```

File Name f-stack-2/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=798
Status New

The variable declared in null at f-stack-2/fm_cc.c in line 5158 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5221	255
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcTreeAddCPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5221.              NULL, &nextEngineParams, h_FmPcd);
```

File Name f-stack-2/fm_cc.c

Method	static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=799
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5149	255
Object	null	h_StatsFLRs

Code Snippet

File Name	f-stack-2/fm_cc.c
Method	t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5149.              NULL, &nextEngineParams, h_FmPcd);
```

File Name	f-stack-2/fm_cc.c
Method	static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=800
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c

Line	4773	255
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4773.              NextStepAd(p_AdTableTmp, NULL, &p_KeyParams-
>ccNextEngineParams,
```

File Name f-stack-2/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=801
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 5994 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6197	255
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6197.          NextStepAd(p_CcTreeTmp, NULL,
```

File Name f-stack-2/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=802
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4815	255
Object	null	h_StatsFLRs

Code Snippet

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4815.           NextStepAd(p_AdTableTmp, NULL,
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=803
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5121	255
Object	null	h_StatsFLRs

Code Snippet

File Name f-stack-2/fm_cc.c

Method	t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5121.                   NULL, &nextEngineParams, h_FmPcd);
```

File Name	f-stack-2/fm_cc.c
Method	static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=804
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	890	239
Object	null	h_StatsFLRs

Code Snippet	
File Name	f-stack-2/fm_cc.c
Method	static t_Handle BuildNewAd(

```
....
890.                   h_Ad, NULL, p_CcNode->h_FmPcd, p_FmPcdCcNodeTmp,
```

File Name	f-stack-2/fm_cc.c
Method	static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=805
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	881	239
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
881.          FillAdOfTypeContLookup(h_Ad, NULL, p_CcNode->h_FmPcd,
p_FmPcdCcNodeTmp,
```

File Name f-stack-2/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=806
Status New

The variable declared in null at f-stack-2/fm_cc.c in line 377 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	403	239
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error AllocAndFillAdForContLookupManip(t_Handle h_CcNode)

```
....
403.          FillAdOfTypeContLookup(p_CcNode->h_Ad, NULL, p_CcNode-
>h_FmPcd,
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=807
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4815	239
Object	null	h_StatsFLRs

Code Snippet

File Name f-stack-2/fm_cc.c

Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4815.          NextStepAd(p_AdTableTmp, NULL,
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=808
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	4773	239
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4773.              NextStepAd(p_AdTableTmp, NULL, &p_KeyParams-
>ccNextEngineParams,
```

File Name f-stack-2/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=809
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 3094 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3239	239
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3239.          NextStepAd(p_Ad, NULL, p_CcNextEngineParams, h_FmPcd);
```

File Name f-stack-2/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=810
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 5994 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	6197	239
Object	null	h_StatsFLRs

Code Snippet

File Name f-stack-2/fm_cc.c

Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6197.          NextStepAd(p_CcTreeTmp, NULL,
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=811
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5149	239

Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5149.               NULL, &nextEngineParams, h_FmPcd);
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=812
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 5158 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5221	239
Object	null	h_StatsFLRs

Code Snippet
File Name f-stack-2/fm_cc.c
Method t_Error FmPcdCcTreeAddCPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5221.               NULL, &nextEngineParams, h_FmPcd);
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 34:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=813
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	5121	239
Object	null	h_StatsFLRs

Code Snippet

File Name f-stack-2/fm_cc.c

Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5121.                   NULL, &nextEngineParams, h_FmPcd);
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=814
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 2566 is not initialized when it is used by h_StatsFLRs at f-stack-2/fm_cc.c in line 225.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	2686	239
Object	null	h_StatsFLRs

Code Snippet

File Name f-stack-2/fm_cc.c

Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2686.                   NextStepAd(p_AdTableNewTmp, NULL,
```

File Name f-stack-2/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=815
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 3551 is not initialized when it is used by params at f-stack-2/fm_cc.c in line 834.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3556	892
Object	null	params

Code Snippet

File Name f-stack-2/fm_cc.c

Method static t_Error UpdatePtrWhichPointOnCrntMdfNode(

```
....
3556.      t_FmPcdCcNextEngineParams *p_NextEngineParams = NULL;
```

File Name f-stack-2/fm_cc.c

Method static t_Handle BuildNewAd(

```
....
892.                   p_FmPcdCcNextEngineParams-
>params.frParams.h_FrmReplic);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=816
Status	New

The variable declared in null at f-stack-2/fm_cc.c in line 3551 is not initialized when it is used by params at f-stack-2/fm_cc.c in line 834.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3556	887
Object	null	params

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error UpdatePtrWhichPointOnCrntMdfNode(

```
....
3556.      t_FmPcdCcNextEngineParams *p_NextEngineParams = NULL;
```

File Name f-stack-2/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
887.               && (p_FmPcdCcNextEngineParams-
>params.frParams.h_FrmReplic))
```

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=817
Status New

The variable declared in null at f-stack-2/fm_cc.c in line 3551 is not initialized when it is used by params at f-stack-2/fm_cc.c in line 834.

	Source	Destination
File	f-stack-2/fm_cc.c	f-stack-2/fm_cc.c
Line	3556	873
Object	null	params

Code Snippet
File Name f-stack-2/fm_cc.c
Method static t_Error UpdatePtrWhichPointOnCrntMdfNode(

```
....
3556.      t_FmPcdCcNextEngineParams *p_NextEngineParams = NULL;
```

File Name	f-stack-2/fm_cc.c
Method	static t_Handle BuildNewAd(

```
....
873.                        p_FmPcdCcNextEngineParams-
>params.ccParams.h_CcNode)
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=818
Status	New

The variable declared in null at f-stack-2/icmp6.c in line 1881 is not initialized when it is used by inp_socket at f-stack-2/icmp6.c in line 1881.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1886	1982
Object	null	inp_socket

Code Snippet

File Name	f-stack-2/icmp6.c
Method	icmp6_rip6_input(struct mbuf **mp, int off)

```
....
1886.       struct inpcb *last = NULL;
....
1982.                                       &last->inp_socket->so_rcv);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=819
Status	New

The variable declared in null at f-stack-2/icmp6.c in line 1881 is not initialized when it is used by inp_socket at f-stack-2/icmp6.c in line 1881.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1886	1973
Object	null	inp_socket

Code Snippet

File Name f-stack-2/icmp6.c
Method icmp6_rip6_input(struct mbuf **mp, int off)

```
....
1886.       struct inpcb *last = NULL;
....
1973.                               &last->inp_socket->so_rcv,
```

NULL Pointer Dereference\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=820
Status New

The variable declared in null at f-stack-2/icmp6.c in line 1881 is not initialized when it is used by inp_socket at f-stack-2/icmp6.c in line 1881.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1886	1971
Object	null	inp_socket

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_rip6_input(struct mbuf **mp, int off)

```
....
1886.       struct inpcb *last = NULL;
....
1971.                           SOCKBUF_LOCK(&last->inp_socket->so_rcv);
```

NULL Pointer Dereference\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=821
Status New

The variable declared in null at f-stack-2/icmp6.c in line 2039 is not initialized when it is used by ip6_src at f-stack-2/icmp6.c in line 2039.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2094	2149
Object	null	ip6_src

Code Snippet

File Name	f-stack-2/icmp6.c
Method	icmp6_reflect(struct mbuf *m, size_t off)

```
....
2094.        srcp = NULL;
....
2149.        ip6->ip6_src = *srcp;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=822
Status	New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1393
Object	null	buf

Code Snippet

File Name	f-stack-2/ngx_http_grpc_module.c
Method	ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1393.                           cl->buf->file_last - cl->buf->file_pos);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=823
Status	New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1393
Object	null	buf

Code Snippet

File Name	f-stack-2/ngx_http_grpc_module.c
Method	ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1393.                           cl->buf->file_last - cl->buf->file_pos);
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=824
Status	New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1392
Object	null	buf

Code Snippet

File Name	f-stack-2/ngx_http_grpc_module.c
Method	ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1392.                           cl->buf->file_pos,
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=825
Status	New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1391
Object	null	buf

Code Snippet

File Name f-stack-2/ngx_http_grpc_module.c
Method ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1391.                           cl->buf->last - cl->buf->pos,
```

NULL Pointer Dereference\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=826
Status New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1391
Object	null	buf

Code Snippet
File Name f-stack-2/ngx_http_grpc_module.c
Method ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1391.                           cl->buf->last - cl->buf->pos,
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=827
Status New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1390
Object	null	buf

Code Snippet

File Name	f-stack-2/ngx_http_grpc_module.c
Method	ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1390.                           cl->buf->start, cl->buf->pos,
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=828
Status	New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1390
Object	null	buf

Code Snippet

File Name	f-stack-2/ngx_http_grpc_module.c
Method	ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1390.                           cl->buf->start, cl->buf->pos,
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=829
Status	New

The variable declared in null at f-stack-2/ngx_http_grpc_module.c in line 1099 is not initialized when it is used by buf at f-stack-2/ngx_http_grpc_module.c in line 1099.

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	1129	1389
Object	null	buf

Code Snippet

File Name	f-stack-2/ngx_http_grpc_module.c
Method	ngx_http_grpc_body_output_filter(void *data, ngx_chain_t *in)

```
....
1129.       out = NULL;
....
1389.                           cl->buf->in_file,
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=686
Status	New

The backgroundRewriteDoneHandler method calls the snprintf function, at line 1851 of f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1864	1864
Object	snprintf	snprintf

Code Snippet

File Name	f-stack-2/aof.c
Method	void backgroundRewriteDoneHandler(int exitcode, int bysignal) {

```
....
1864.           snprintf(tmpfile,256,"temp-rewriteaof-bg-%d.aof",
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=687
Status	New

The feedAppendOnlyFile method calls the snprintf function, at line 613 of f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	620	620
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/aof.c
Method void feedAppendOnlyFile(struct redisCommand *cmd, int dictid, robj **argv, int argc) {

```
....
620.          snprintf(seldb,sizeof(seldb),"%d",dictid);
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=688
Status New

The rewriteAppendOnlyFile method calls the snprintf function, at line 1546 of f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1554	1554
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteAppendOnlyFile(char *filename) {

```
....
1554.      snprintf(tmpfile,256,"temp-rewriteaof-%d.aof", (int)
getpid());
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=689
Status New

The rewriteAppendOnlyFileBackground method calls the snprintf function, at line 1763 of f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1774	1774
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteAppendOnlyFileBackground(void) {

```
....
1774.           snprintf(tmpfile,256,"temp-rewriteaof-bg-%d.aof", (int)
getpid());
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=690
Status New

The aofRemoveTempFile method calls the snprintf function, at line 1820 of f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1823	1823
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/aof.c
Method void aofRemoveTempFile(pid_t childpid) {

```
....
1823.       snprintf(tmpfile,256,"temp-rewriteaof-bg-%d.aof", (int)
childpid);
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=691
Status New

The aofRemoveTempFile method calls the snprintf function, at line 1820 of f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1826	1826
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/aof.c
Method void aofRemoveTempFile(pid_t childpid) {

```
....
1826.       snprintf(tmpfile,256,"temp-rewriteaof-%d.aof", (int)
childpid);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=692
Status New

The bcmfs_queue_create method calls the snprintf function, at line 95 of f-stack-2/bcmfs_qp.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	f-stack-2/bcmfs_qp.c	f-stack-2/bcmfs_qp.c
Line	133	133
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/bcmfs_qp.c
Method bcmfs_queue_create(struct bcmfs_queue *queue,

```
....
133.        snprintf(queue->memz_name, sizeof(queue->memz_name),
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=693
Status New

The __pip_eth_node method calls the sprintf function, at line 107 of f-stack-2/cvmx-helper-board.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	f-stack-2/cvmx-helper-board.c	f-stack-2/cvmx-helper-board.c
Line	128	128
Object	sprintf	sprintf

Code Snippet
File Name f-stack-2/cvmx-helper-board.c
Method static int __pip_eth_node(const void *fdt_addr, int aliases, int ipd_port)

```
....
128.      sprintf(name_buffer, "interface@%d", interface_num);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=694
Status New

The __pip_eth_node method calls the sprintf function, at line 107 of f-stack-2/cvmx-helper-board.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	f-stack-2/cvmx-helper-board.c	f-stack-2/cvmx-helper-board.c
Line	140	140
Object	sprintf	sprintf

Code Snippet
File Name f-stack-2/cvmx-helper-board.c
Method static int __pip_eth_node(const void *fdt_addr, int aliases, int ipd_port)

```
....
140.      sprintf(name_buffer, "ethernet@%x", interface_index);
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=695
Status New

The __mix_eth_node method calls the sprintf function, at line 154 of f-stack-2/cvmx-helper-board.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	f-stack-2/cvmx-helper-board.c	f-stack-2/cvmx-helper-board.c
Line	161	161
Object	sprintf	sprintf

Code Snippet
File Name f-stack-2/cvmx-helper-board.c
Method static int __mix_eth_node(const void *fdt_addr, int aliases, int interface_index)

```
....
161.      sprintf(name_buffer, "mix%d", interface_index);
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=696
Status New

The cbor_memdump method calls the sprintf function, at line 39 of f-stack-2/enc_cbor.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	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	70	70
Object	sprintf	sprintf

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_memdump (FILE *fp, const char *title, const char *data,

```
....
70.              sprintf(bp, "%02x ", (unsigned char) *data);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=697
Status New

The icmp6_redirect_diag method calls the snprintf function, at line 2192 of f-stack-2/icmp6.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	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2199	2199
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_diag(struct in6_addr *src6, struct in6_addr *dst6,

```
....
2199.       snprintf(buf, sizeof(buf), "(src=%s dst=%s tgt=%s)",
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=698
Status New

The rte_ethtool_get_drvinfo method calls the snprintf function, at line 22 of f-stack-2/rte_ethtool.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	f-stack-2/rte_ethtool.c	f-stack-2/rte_ethtool.c
Line	60	60
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/rte_ethtool.c
Method rte_ethtool_get_drvinfo(uint16_t port_id, struct ethtool_drvinfo *drvinfo)

```
....
60.         snprintf(drvinfo->bus_info, sizeof(drvinfo->bus_info),
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=699
Status New

The rte_ethtool_get_drvinfo method calls the snprintf function, at line 22 of f-stack-2/rte_ethtool.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	f-stack-2/rte_ethtool.c	f-stack-2/rte_ethtool.c
Line	65	65
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/rte_ethtool.c
Method rte_ethtool_get_drvinfo(uint16_t port_id, struct ethtool_drvinfo *drvinfo)

```
....
65.         snprintf(drvinfo->bus_info, sizeof(drvinfo->bus_info),
"N/A");
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=700
Status New

The sentinelEvent method calls the snprintf function, at line 694 of f-stack-2/sentinel.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	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	706	706
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
706.             snprintf(msg, sizeof(msg), "%s %s %s %d @ %s %s %d",
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=701
Status New

The sentinelEvent method calls the snprintf function, at line 694 of f-stack-2/sentinel.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	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	711	711
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
711.              snprintf(msg, sizeof(msg), "%s %s %s %d",
```

Unchecked Return Value\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=702
Status New

The sentinelSetClientName method calls the snprintf function, at line 2384 of f-stack-2/sentinel.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	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	2387	2387
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelSetClientName(sentinelRedisInstance *ri, redisAsyncContext *c, char *type) {

```
....
2387.      snprintf(name,sizeof(name),"sentinel-%.8s-
%s",sentinel.myid,type);
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=703
Status New

The sentinelSendHello method calls the snprintf function, at line 2990 of f-stack-2/sentinel.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	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	3015	3015
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method int sentinelSendHello(sentinelRedisInstance *ri) {

```
....
3015.       snprintf(payload,sizeof(payload),
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=704
Status New

The create_mbuf_pool method calls the snprintf function, at line 462 of f-stack-2/test_bbdev_perf.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	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	475	475
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method create_mbuf_pool(struct op_data_entries *entries, uint8_t dev_id,

```
....
475.         snprintf(pool_name, sizeof(pool_name), "%s_pool_%u",
op_type_str,
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=705
Status New

The create_mempools method calls the snprintf function, at line 484 of f-stack-2/test_bbdev_perf.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	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	518	518
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method create_mempools(struct active_device *ad, int socket_id,

```
....
518.         snprintf(pool_name, sizeof(pool_name), "%s_pool_%u",
op_type_str,
```

Unchecked Return Value\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=706
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	109	109
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
109.                     snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=707
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	118	118
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
118.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=708
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	131	131
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
131.                            snprintf(test_msg,
BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=709
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	140	140
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
140.                            snprintf(test_msg,
BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=710
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	150	150
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
150.                snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=711
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	159	159
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
159.                snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"SKIPPED");
```

Unchecked Return Value\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=712
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	171	171
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
171.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=713
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	178	178
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
178.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"SKIPPED");
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=714
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	196	196
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
196.                snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"SKIPPED");
```

Unchecked Return Value\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=715
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	212	212
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
212.                snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=716
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	243	243
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
243.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=717
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	261	261
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
261.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=718
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	274	274
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
274.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=719
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	286	286
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
286.              snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=720
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	329	329
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
329.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=721
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	362	362
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
362.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=722
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	376	376
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
376.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=723
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	442	442
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
442.                snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=724
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	522	522
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
522.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"UNSUPPORTED");
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=725
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	527	527
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
527.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=726
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	561	561
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
561.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=727
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	574	574
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
574.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=728
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	592	592
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
592.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=729
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	596	596
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
596.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=730
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	625	625
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
625.                    snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN,
"line %u "
```

Unchecked Return Value\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=731
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	644	644
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
644.                            snprintf(test_msg,
BLOCKCIPHER_TEST_MSG_LEN, "line %u "
```

Unchecked Return Value\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=732
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	691	691
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
691.                            snprintf(test_msg,
BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=733
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	721	721
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
721.                            snprintf(test_msg,
BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=734
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	790	790
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
790.                            snprintf(test_msg,
BLOCKCIPHER_TEST_MSG_LEN,
```

Unchecked Return Value\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=735
Status New

The test_blockcipher_one_case method calls the snprintf function, at line 67 of f-stack-2/test_cryptodev_blockcipher.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	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	800	800
Object	snprintf	snprintf

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method test_blockcipher_one_case(const struct blockcipher_test_case *t,

```
....
800.        snprintf(test_msg, BLOCKCIPHER_TEST_MSG_LEN, "PASS");
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=743
Status New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	835	835
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
835.          argv = zmalloc(sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=744
Status New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	626	626

Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/bitops.c
Method void bitopCommand(client *c) {

```
....
626.      src = zmalloc(sizeof(unsigned char*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=745
Status New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	628	628
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/bitops.c
Method void bitopCommand(client *c) {

```
....
628.      objects = zmalloc(sizeof(robj*) * numkeys);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=746
Status New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	676	676
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/bitops.c
Method void bitopCommand(client *c) {

```
....
676.              memcpy(lp,src,sizeof(unsigned long*)*numkeys);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=747
Status	New

	Source	Destination
File	f-stack-2/enic_rxtx_vec_avx2.c	f-stack-2/enic_rxtx_vec_avx2.c
Line	788	788
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/enic_rxtx_vec_avx2.c
Method enic_noscatter_vec_recv_pkts(void *rx_queue, struct rte_mbuf **rx_pkts,

```
....
788.               sizeof(struct rte_mbuf *) * nb_rx);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=748
Status	New

	Source	Destination
File	f-stack-2/lobject.c	f-stack-2/lobject.c
Line	144	144
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/lobject.c
Method const char *luaO_pushvfstring (lua_State *L, const char *fmt, va_list argp) {

```
....
144.          char buff[4*sizeof(void *) + 8]; /* should be enough space
for a `%p' */
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=749
Status	New

	Source	Destination
File	f-stack-2/multi.c	f-stack-2/multi.c
Line	74	74
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/multi.c
Method void queueMultiCommand(client *c) {

```
....
74.      mc->argv = zmalloc(sizeof(robj*)*c->argc);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=750
Status	New

	Source	Destination
File	f-stack-2/multi.c	f-stack-2/multi.c
Line	75	75
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/multi.c
Method void queueMultiCommand(client *c) {

```
....
75.      memcpy(mc->argv,c->argv,sizeof(robj*)*c->argc);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=751
Status	New

	Source	Destination
File	f-stack-2/ngx_http_ssi_filter_module.c	f-stack-2/ngx_http_ssi_filter_module.c

Line	741	741
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_ssi_filter_module.c
Method ngx_http_ssi_body_filter(ngx_http_request_t *r, ngx_chain_t *in)

```
....
741.                                (NGX_HTTP_SSI_MAX_PARAMS + 1) *
sizeof(ngx_str_t *));
```

Use of Sizeof On a Pointer Type\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=752
Status New

	Source	Destination
File	f-stack-2/ngx_http_ssi_filter_module.c	f-stack-2/ngx_http_ssi_filter_module.c
Line	1693	1693
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_ssi_filter_module.c
Method ngx_http_ssi_evaluate_string(ngx_http_request_t *r, ngx_http_ssi_ctx_t *ctx,

```
....
1693.       if (ngx_array_init(&lengths, r->pool, 8, sizeof(size_t *)) !=
NGX_OK) {
```

Use of Sizeof On a Pointer Type\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=753
Status New

	Source	Destination
File	f-stack-2/ngx_http_ssi_filter_module.c	f-stack-2/ngx_http_ssi_filter_module.c
Line	1697	1697
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_ssi_filter_module.c
Method ngx_http_ssi_evaluate_string(ngx_http_request_t *r, ngx_http_ssi_ctx_t *ctx,

```
....
1697.      if (ngx_array_init(&values, r->pool, 8, sizeof(u_char *)) !=
NGX_OK) {
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=754
Status	New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4532	4532
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_process_set_cookie(ngx_http_request_t *r, ngx_table_elt_t *h,

```
....
4532.          if (ngx_array_init(pa, r->pool, 1, sizeof(ngx_table_elt_t
*)) != NGX_OK)
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=755
Status	New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4567	4567
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_process_cache_control(ngx_http_request_t *r,

```
....
4567.          if (ngx_array_init(pa, r->pool, 2, sizeof(ngx_table_elt_t
*)) != NGX_OK)
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=756
Status	New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	4966	4966
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_copy_multi_header_lines(ngx_http_request_t *r,

```
....
4966.          if (ngx_array_init(pa, r->pool, 2, sizeof(ngx_table_elt_t
*)) != NGX_OK)
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=757
Status	New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	5737	5737
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream(ngx_conf_t *cf, ngx_command_t *cmd, void *dummy)

```
....
5737.      ctx->srv_conf = ngx_pcalloc(cf->pool, sizeof(void *) *
ngx_http_max_module);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=758
Status	New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	5749	5749
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream(ngx_conf_t *cf, ngx_command_t *cmd, void *dummy)

```
....
5749.      ctx->loc_conf = ngx_pcalloc(cf->pool, sizeof(void *) *
ngx_http_max_module);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=759
Status New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	6410	6410
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream_create_main_conf(ngx_conf_t *cf)

```
....
6410.                          sizeof(ngx_http_upstream_srv_conf_t *))
```

Use of Sizeof On a Pointer Type\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=760
Status New

	Source	Destination
File	f-stack-2/ngx_http_uwsgi_module.c	f-stack-2/ngx_http_uwsgi_module.c
Line	902	902
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_uwsgi_module.c
Method ngx_http_uwsgi_create_request(ngx_http_request_t *r)

```
....
902.              ignored = ngx_palloc(r->pool, n * sizeof(void *));
```

Use of Sizeof On a Pointer Type\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=761
Status New

	Source	Destination
File	f-stack-2/ngx_http_uwsgi_module.c	f-stack-2/ngx_http_uwsgi_module.c
Line	1390	1390
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_http_uwsgi_module.c
Method ngx_http_uwsgi_create_main_conf(ngx_conf_t *cf)

```
....
1390.                           sizeof(ngx_http_file_cache_t *))
```

Use of Sizeof On a Pointer Type\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=762
Status New

	Source	Destination
File	f-stack-2/ngx_stream_core_module.c	f-stack-2/ngx_stream_core_module.c
Line	368	368
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_stream_core_module.c
Method ngx_stream_core_create_main_conf(ngx_conf_t *cf)

```
....
368.                           sizeof(ngx_stream_core_srv_conf_t *))
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=763
Status	New

	Source	Destination
File	f-stack-2/ngx_stream_core_module.c	f-stack-2/ngx_stream_core_module.c
Line	534	534
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_stream_core_module.c
Method ngx_stream_core_server(ngx_conf_t *cf, ngx_command_t *cmd, void *conf)

```
....
534.                                    sizeof(void *) *
ngx_stream_max_module);
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=764
Status	New

	Source	Destination
File	f-stack-2/ngx_string.c	f-stack-2/ngx_string.c
Line	429	429
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/ngx_string.c
Method ngx_vslprintf(u_char *buf, u_char *last, const char *fmt, va_list args)

```
....
429.                    width = 2 * sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=765
Status	New

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	1091	1091
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/sds.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1091.               vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=766
Status New

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	1097	1097
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/sds.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1097.               if (vector == NULL) vector = s_malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=767
Status New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	798	798
Object	sizeof	sizeof

Code Snippet

File Name	f-stack-2/sentinel.c
Method	void sentinelScheduleScriptExecution(char *path, ...) {

```
....
798.      sj->argv = zmalloc(sizeof(char*)*(argc+1));
```

Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=768
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	801	801
Object	sizeof	sizeof

Code Snippet

File Name	f-stack-2/sentinel.c
Method	void sentinelScheduleScriptExecution(char *path, ...) {

```
....
801.      memcpy(sj->argv,argv,sizeof(char*)*(argc+1));
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=769
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	1638	1638
Object	sizeof	sizeof

Code Snippet

File Name	f-stack-2/sentinel.c
Method	int sentinelResetMasterAndChangeAddress(sentinelRedisInstance *master, char *hostname, int port) {

```
....
1638.      slaves = zmalloc(sizeof(sentinelAddr*)*(dictSize(master-
>slaves) + 1));
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=770
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	1821	1821
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/sentinel.c
Method void queueSentinelConfig(sds *argv, int argc, int linenum, sds line) {

```
....
1821.       entry->argv = zmalloc(sizeof(char*)*argc);
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=771
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	4727	4727
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/sentinel.c
Method sentinelRedisInstance *sentinelSelectSlave(sentinelRedisInstance *master) {

```
....
4727.           qsort(instance,instances,sizeof(sentinelRedisInstance*),
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=772
Status	New

	Source	Destination
File	f-stack-2/t_set.c	f-stack-2/t_set.c
Line	857	857
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/t_set.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
857.      robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=773
Status New

	Source	Destination
File	f-stack-2/t_set.c	f-stack-2/t_set.c
Line	902	902
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/t_set.c
Method void sinterGenericCommand(client *c, robj **setkeys,

```
....
902.
qsort(sets,setnum,sizeof(robj*),qsortCompareSetsByCardinality);
```

Use of Sizeof On a Pointer Type\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=774
Status New

	Source	Destination
File	f-stack-2/t_set.c	f-stack-2/t_set.c
Line	1009	1009
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/t_set.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
1009.       robj **sets = zmalloc(sizeof(robj*)*setnum);
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=775
Status	New

	Source	Destination
File	f-stack-2/t_set.c	f-stack-2/t_set.c
Line	1059	1059
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/t_set.c
Method void sunionDiffGenericCommand(client *c, robj **setkeys, int setnum,

```
....
1059.               qsort(sets+1,setnum-1,sizeof(robj*),
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=776
Status	New

	Source	Destination
File	f-stack-2/t_stream.c	f-stack-2/t_stream.c
Line	2037	2037
Object	sizeof	sizeof

Code Snippet
File Name f-stack-2/t_stream.c
Method void xreadCommand(client *c) {

```
....
2037.       if (groupname) groups =
zmalloc(sizeof(streamCG*)*streams_count);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=927
Status	New

Method icmp6_input in f-stack-2/icmp6.c, at line 397, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	563	563
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
563.                    bcopy(ip6, nip6, sizeof(struct ip6_hdr));
```

Use of Obsolete Functions\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=928
Status	New

Method icmp6_input in f-stack-2/icmp6.c, at line 397, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	565	565
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
565.                    bcopy(icmp6, nicmp6, sizeof(struct icmp6_hdr));
```

Use of Obsolete Functions\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=929
Status	New

Method icmp6_input in f-stack-2/icmp6.c, at line 397, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	701	701
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
701.                    bcopy(ip6, nip6, sizeof(struct ip6_hdr));
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=930
Status	New

Method icmp6_input in f-stack-2/icmp6.c, at line 397, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	703	703
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
703.                    bcopy(icmp6, nicmp6, sizeof(struct icmp6_hdr));
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=931
Status	New

Method icmp6_input in f-stack-2/icmp6.c, at line 397, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	714	714
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
714.                    bcopy(pr->pr_hostname, p + 4, maxhlen);
```

Use of Obsolete Functions\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=932
Status	New

Method ni6_input in f-stack-2/icmp6.c, at line 1171, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1421	1421
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_input(struct mbuf *m, int off, struct prison *pr)

```
....
1421.       bcopy(mtod(m, caddr_t), mtod(n, caddr_t), sizeof(struct
ip6_hdr));
```

Use of Obsolete Functions\Path 7:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=933
Status	New

Method ni6_input in f-stack-2/icmp6.c, at line 1171, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1423	1423
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_input(struct mbuf *m, int off, struct prison *pr)

```
....
1423.       bcopy((caddr_t)ni6, (caddr_t)nni6, sizeof(struct
icmp6_nodeinfo));
```

Use of Obsolete Functions\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=934
Status	New

Method ni6_input in f-stack-2/icmp6.c, at line 1171, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1438	1438
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_input(struct mbuf *m, int off, struct prison *pr)

```
....
1438.             bcopy(&v, nni6 + 1, sizeof(u_int32_t));
```

Use of Obsolete Functions\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=935
Status	New

Method ni6_nametodns in f-stack-2/icmp6.c, at line 1499, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1563	1563
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_nametodns(const char *name, int namelen, int old)

```
....
1563.                   bcopy(p, cp, i);
```

Use of Obsolete Functions\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=936
Status	New

Method ni6_store_addrs in f-stack-2/icmp6.c, at line 1743, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1851	1851
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1851.                   bcopy(&ltime, cp, sizeof(u_int32_t));
```

Use of Obsolete Functions\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=937
Status	New

Method ni6_store_addrs in f-stack-2/icmp6.c, at line 1743, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination

File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1855	1855
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1855.                    bcopy(&ifa6->ia_addr.sin6_addr, cp,
```

Use of Obsolete Functions\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=938
Status New

Method icmp6_rip6_input in f-stack-2/icmp6.c, at line 1881, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	1956	1956
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_rip6_input(struct mbuf **mp, int off)

```
....
1956.                                    bcopy(m->m_data, n->m_data,
```

Use of Obsolete Functions\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=939
Status New

Method icmp6_rip6_input in f-stack-2/icmp6.c, at line 1881, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2005	2005
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_rip6_input(struct mbuf **mp, int off)

```
....
2005.                                   bcopy(m->m_data, n->m_data, m-
>m_len);
```

Use of Obsolete Functions\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=940
Status	New

Method icmp6_reflect in f-stack-2/icmp6.c, at line 2039, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2078	2078
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_reflect(struct mbuf *m, size_t off)

```
....
2078.             bcopy((caddr_t)&nip6, mtod(m, caddr_t), sizeof(nip6));
```

Use of Obsolete Functions\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=941
Status	New

Method icmp6_redirect_input in f-stack-2/icmp6.c, at line 2206, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2378	2378
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_input(struct mbuf *m, int off)

```
....
2378.             bcopy(&reddst6, &sdst.sin6_addr, sizeof(struct
in6_addr));
```

Use of Obsolete Functions\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=942
Status	New

Method icmp6_redirect_input in f-stack-2/icmp6.c, at line 2206, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2379	2379
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_input(struct mbuf *m, int off)

```
....
2379.             bcopy(&src6, &ssrc.sin6_addr, sizeof(struct
in6_addr));
```

Use of Obsolete Functions\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=943
Status	New

Method icmp6_redirect_input in f-stack-2/icmp6.c, at line 2206, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2385	2385
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_input(struct mbuf *m, int off)

```
....
2385.                   bcopy(&redtgt6, &sgw.sin6_addr,
```

Use of Obsolete Functions\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=944
Status	New

Method icmp6_redirect_input in f-stack-2/icmp6.c, at line 2206, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2403	2403
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_input(struct mbuf *m, int off)

```
....
2403.       bcopy(&reddst6, &sdst.sin6_addr, sizeof(struct in6_addr));
```

Use of Obsolete Functions\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=945
Status	New

Method icmp6_redirect_output in f-stack-2/icmp6.c, at line 2417, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2514	2514
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2514.       bcopy(ifp_ll6, &ip6->ip6_src, sizeof(struct in6_addr));
```

Use of Obsolete Functions\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=946
Status	New

Method icmp6_redirect_output in f-stack-2/icmp6.c, at line 2417, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2515	2515
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2515.       bcopy(&sip6->ip6_src, &ip6->ip6_dst, sizeof(struct
in6_addr));
```

Use of Obsolete Functions\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=947
Status	New

Method icmp6_redirect_output in f-stack-2/icmp6.c, at line 2417, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2529	2529
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2529.             bcopy(router_ll6, &nd_rd->nd_rd_target,
```

Use of Obsolete Functions\Path 22:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=948
Status	New

Method icmp6_redirect_output in f-stack-2/icmp6.c, at line 2417, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2531	2531
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2531.             bcopy(&sip6->ip6_dst, &nd_rd->nd_rd_dst,
```

Use of Obsolete Functions\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=949
Status	New

Method icmp6_redirect_output in f-stack-2/icmp6.c, at line 2417, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2535	2535
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2535.             bcopy(&sip6->ip6_dst, &nd_rd->nd_rd_target,
```

Use of Obsolete Functions\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=950
Status	New

Method icmp6_redirect_output in f-stack-2/icmp6.c, at line 2417, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2537	2537
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2537.             bcopy(&sip6->ip6_dst, &nd_rd->nd_rd_dst,
```

Use of Obsolete Functions\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=951
Status	New

Method icmp6_redirect_output in f-stack-2/icmp6.c, at line 2417, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	f-stack-2/icmp6.c	f-stack-2/icmp6.c
Line	2567	2567
Object	bcopy	bcopy

Code Snippet
File Name f-stack-2/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2567.                   bcopy(ln->ll_addr, lladdr, ifp->if_addrlen);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=300

	36&pathid=958
Status	New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	219	219
Object	byte	byte

Code Snippet
File Name f-stack-2/bitops.c
Method void setUnsignedBitfield(unsigned char *p, uint64_t offset, uint64_t bits, uint64_t value) {

```
....
219.          p[byte] = byteval & 0xff;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=959
Status	New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	558	558
Object	byte	byte

Code Snippet
File Name f-stack-2/bitops.c
Method void setbitCommand(client *c) {

```
....
558.      ((uint8_t*)o->ptr)[byte] = byteval;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=960
Status	New

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1754	1754

Object	num	num

Code Snippet
File Name f-stack-2/db.c
Method int sortGetKeys(struct redisCommand *cmd, robj **argv, int argc, getKeysResult *result) {

```
....
1754.                   keys[num] = i+1; /* <store-key> */
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=961
Status New

	Source	Destination
File	f-stack-2/db.c	f-stack-2/db.c
Line	1922	1922
Object	hashslot	hashslot

Code Snippet
File Name f-stack-2/db.c
Method void slotToKeyUpdateKey(sds key, int add) {

```
....
1922.       server.cluster->slots_keys_count[hashslot] += add ? 1 : -1;
```

Unchecked Array Index\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=962
Status New

	Source	Destination
File	f-stack-2/listpack.c	f-stack-2/listpack.c
Line	513	513
Object	lp	lp

Code Snippet
File Name f-stack-2/listpack.c
Method uint32_t lpLength(unsigned char *lp) {

```
....
513.      if (count < LP_HDR_NUMELE_UNKNOWN) lpSetNumElements(lp,count);
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=963
Status	New

	Source	Destination
File	f-stack-2/listpack.c	f-stack-2/listpack.c
Line	513	513
Object	lp	lp

Code Snippet
File Name f-stack-2/listpack.c
Method uint32_t lpLength(unsigned char *lp) {

```
....
513.      if (count < LP_HDR_NUMELE_UNKNOWN) lpSetNumElements(lp,count);
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=964
Status	New

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	3010	3010
Object	len	len

Code Snippet
File Name f-stack-2/ngx_http_grpc_module.c
Method ngx_http_grpc_parse_fragment(ngx_http_request_t *r, ngx_http_grpc_ctx_t *ctx,

```
....
3010.                  ctx->name.data[ctx->name.len] = '\0';
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=965
Status	New

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	3014	3014
Object	len	len

Code Snippet
File Name f-stack-2/ngx_http_grpc_module.c
Method ngx_http_grpc_parse_fragment(ngx_http_request_t *r, ngx_http_grpc_ctx_t *ctx,

```
....
3014.                    ctx->name.data[ctx->name.len] = '\0';
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=966
Status	New

	Source	Destination
File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	3119	3119
Object	len	len

Code Snippet
File Name f-stack-2/ngx_http_grpc_module.c
Method ngx_http_grpc_parse_fragment(ngx_http_request_t *r, ngx_http_grpc_ctx_t *ctx,

```
....
3119.                    ctx->value.data[ctx->value.len] = '\0';
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=967
Status	New

	Source	Destination

File	f-stack-2/ngx_http_grpc_module.c	f-stack-2/ngx_http_grpc_module.c
Line	3123	3123
Object	len	len

Code Snippet
File Name f-stack-2/ngx_http_grpc_module.c
Method ngx_http_grpc_parse_fragment(ngx_http_request_t *r, ngx_http_grpc_ctx_t *ctx,

```
....
3123.                    ctx->value.data[ctx->value.len] = '\0';
```

Unchecked Array Index\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=968
Status New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	5742	5742
Object	ctx_index	ctx_index

Code Snippet
File Name f-stack-2/ngx_http_upstream.c
Method ngx_http_upstream(ngx_conf_t *cf, ngx_command_t *cmd, void *dummy)

```
....
5742.      ctx->srv_conf[ngx_http_upstream_module.ctx_index] = uscf;
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=969
Status New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	5767	5767
Object	ctx_index	ctx_index

Code Snippet
File Name f-stack-2/ngx_http_upstream.c

Method	ngx_http_upstream(ngx_conf_t *cf, ngx_command_t *cmd, void *dummy)

```
....
5767.                ctx->srv_conf[cf->cycle->modules[m]->ctx_index] =
mconf;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=970
Status	New

	Source	Destination
File	f-stack-2/ngx_http_upstream.c	f-stack-2/ngx_http_upstream.c
Line	5776	5776
Object	ctx_index	ctx_index

Code Snippet	
File Name	f-stack-2/ngx_http_upstream.c
Method	ngx_http_upstream(ngx_conf_t *cf, ngx_command_t *cmd, void *dummy)

```
....
5776.                ctx->loc_conf[cf->cycle->modules[m]->ctx_index] =
mconf;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=971
Status	New

	Source	Destination
File	f-stack-2/ngx_http_uwsgi_module.c	f-stack-2/ngx_http_uwsgi_module.c
Line	1270	1270
Object	len	len

Code Snippet	
File Name	f-stack-2/ngx_http_uwsgi_module.c
Method	ngx_http_uwsgi_process_header(ngx_http_request_t *r)

```
....
1270.                h->value.data[h->value.len] = '\0';
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=972
Status	New

	Source	Destination
File	f-stack-2/ngx_stream_core_module.c	f-stack-2/ngx_stream_core_module.c
Line	552	552
Object	ctx_index	ctx_index

Code Snippet
File Name f-stack-2/ngx_stream_core_module.c
Method ngx_stream_core_server(ngx_conf_t *cf, ngx_command_t *cmd, void *conf)

```
....
552.                ctx->srv_conf[cf->cycle->modules[m]->ctx_index] =
mconf;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=973
Status	New

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	406	406
Object	len	len

Code Snippet
File Name f-stack-2/sds.c
Method void sdsIncrLen(sds s, ssize_t incr) {

```
....
406.      s[len] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=974
Status	New

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	729	729
Object	i	i

Code Snippet
File Name f-stack-2/sds.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
729.        s[i] = '\0';
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=975
Status New

	Source	Destination
File	f-stack-2/sds.c	f-stack-2/sds.c
Line	757	757
Object	len	len

Code Snippet
File Name f-stack-2/sds.c
Method sds sdstrim(sds s, const char *cset) {

```
....
757.        s[len] = '\0';
```

Unchecked Array Index\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=976
Status New

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	349	349
Object	next	next

Code Snippet

File Name	f-stack-2/util.c
Method	int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
349.      dst[next] = '\0';
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=977
Status	New

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	354	354
Object	next	next

Code Snippet

File Name	f-stack-2/util.c
Method	int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
354.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=978
Status	New

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	361	361
Object	next	next

Code Snippet

File Name	f-stack-2/util.c
Method	int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
361.          dst[next] = '0' + (uint32_t) value;
```

Unchecked Array Index\Path 22:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=979
Status	New

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	364	364
Object	next	next

Code Snippet
File Name f-stack-2/util.c
Method int ll2string(char *dst, size_t dstlen, long long svalue) {

```
....
364.          dst[next] = digits[i + 1];
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=980
Status	New

	Source	Destination
File	f-stack-2/vhost.c	f-stack-2/vhost.c
Line	733	733
Object	vid	vid

Code Snippet
File Name f-stack-2/vhost.c
Method vhost_destroy_device(int vid)

```
....
733.        vhost_devices[vid] = NULL;
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=651
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	822	822
Object	fgets	fgets

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
822.          if (fgets(buf,sizeof(buf),fp) == NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=652
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	841	841
Object	fgets	fgets

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
841.              char *readres = fgets(buf,sizeof(buf),fp);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=653
Status	New

	Source	Destination

File	f-stack-2/aof.c	f-stack-2/aof.c
Line	822	822
Object	buf	buf

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
822.          if (fgets(buf,sizeof(buf),fp) == NULL) {
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=654
Status New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	841	841
Object	buf	buf

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
841.              char *readres = fgets(buf,sizeof(buf),fp);
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=655
Status New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	788	788
Object	sig	sig

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
788.      if (fread(sig,1,5,fp) != 5 || memcmp(sig,"REDIS",5) != 0) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=656
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	854	854
Object	argsds	argsds

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
854.              if (len && fread(argsds,len,1,fp) == 0) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=657
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	863	863
Object	buf	buf

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
863.              if (fread(buf,2,1,fp) == 0) {
```

Improper Resource Access Authorization\Path 8:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=658
Status	New

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	659	659
Object	seed	seed

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
659.          if (fp == NULL || fread(seed,sizeof(seed),1,fp) != 1) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=659
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1444	1444
Object	buf	buf

Code Snippet
File Name f-stack-2/aof.c
Method ssize_t aofReadDiffFromParent(void) {

```
....
1444.
read(server.aof_pipe_read_data_from_parent,buf,sizeof(buf))) > 0) {
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=660
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c

Line	1686	1686
Object	Address	Address

Code Snippet
File Name f-stack-2/aof.c
Method void aofChildPipeReadable(aeEventLoop *el, int fd, void *privdata, int mask) {

```
....
1686.       if (read(fd,&byte,1) == 1 && byte == '!') {
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=661
Status New

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	57	57
Object	fprintf	fprintf

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_memdump (FILE *fp, const char *title, const char *data,

```
....
57.       fprintf(fp, "%*s[%s] @ %p (%lx/%lu)\n", indent + 1, tag,
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=662
Status New

	Source	Destination
File	f-stack-2/enc_cbor.c	f-stack-2/enc_cbor.c
Line	78	78
Object	fprintf	fprintf

Code Snippet
File Name f-stack-2/enc_cbor.c
Method cbor_memdump (FILE *fp, const char *title, const char *data,

```
....
78.          fprintf(fp, "%*s%-54s%s\n", indent + 1, tag, buf, text);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=663
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	1893	1893
Object	fprintf	fprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method void loadSentinelConfigFromQueue(void) {

```
....
1893.      fprintf(stderr, "\n*** FATAL CONFIG FILE ERROR (Redis %s) ***\n",
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=664
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	1895	1895
Object	fprintf	fprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method void loadSentinelConfigFromQueue(void) {

```
....
1895.      fprintf(stderr, "Reading the configuration file, at line %d\n", linenum);
```

Improper Resource Access Authorization\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=665
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	1896	1896
Object	fprintf	fprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method void loadSentinelConfigFromQueue(void) {

```
....
1896.       fprintf(stderr, ">>> '%s'\n", line);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=666
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	1897	1897
Object	fprintf	fprintf

Code Snippet
File Name f-stack-2/sentinel.c
Method void loadSentinelConfigFromQueue(void) {

```
....
1897.       fprintf(stderr, "%s\n", err);
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description
Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=671
Status	New

Method *lwDrawSchotter at line 71 of f-stack-2/lolwut5.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/lolwut5.c	f-stack-2/lolwut5.c
Line	87	87
Object	rand	rand

Code Snippet
File Name f-stack-2/lolwut5.c
Method lwCanvas *lwDrawSchotter(int console_cols, int squares_per_row, int squares_per_col) {

```
....
87.                 float r1 = (float)rand() / (float) RAND_MAX /
squares_per_col * y;
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=672
Status	New

Method *lwDrawSchotter at line 71 of f-stack-2/lolwut5.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/lolwut5.c	f-stack-2/lolwut5.c
Line	88	88
Object	rand	rand

Code Snippet
File Name f-stack-2/lolwut5.c
Method lwCanvas *lwDrawSchotter(int console_cols, int squares_per_row, int squares_per_col) {

```
....
88.                 float r2 = (float)rand() / (float) RAND_MAX /
squares_per_col * y;
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=673
Status	New

Method *lwDrawSchotter at line 71 of f-stack-2/lolwut5.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/lolwut5.c	f-stack-2/lolwut5.c
Line	89	89
Object	rand	rand

Code Snippet
File Name f-stack-2/lolwut5.c
Method lwCanvas *lwDrawSchotter(int console_cols, int squares_per_row, int squares_per_col) {

```
....
89.                 float r3 = (float)rand() / (float) RAND_MAX /
squares_per_col * y;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=674
Status	New

Method *lwDrawSchotter at line 71 of f-stack-2/lolwut5.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/lolwut5.c	f-stack-2/lolwut5.c
Line	90	90
Object	rand	rand

Code Snippet
File Name f-stack-2/lolwut5.c
Method lwCanvas *lwDrawSchotter(int console_cols, int squares_per_row, int squares_per_col) {

```
....
90.                 if (rand() % 2) r1 = -r1;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=675
Status	New

Method *lwDrawSchotter at line 71 of f-stack-2/lolwut5.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/lolwut5.c	f-stack-2/lolwut5.c
Line	91	91
Object	rand	rand

Code Snippet
File Name f-stack-2/lolwut5.c
Method lwCanvas *lwDrawSchotter(int console_cols, int squares_per_row, int squares_per_col) {

```
....
91.                 if (rand() % 2) r2 = -r2;
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=676
Status	New

Method *lwDrawSchotter at line 71 of f-stack-2/lolwut5.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/lolwut5.c	f-stack-2/lolwut5.c
Line	92	92
Object	rand	rand

Code Snippet
File Name f-stack-2/lolwut5.c
Method lwCanvas *lwDrawSchotter(int console_cols, int squares_per_row, int squares_per_col) {

```
....
92.                 if (rand() % 2) r3 = -r3;
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=677
Status	New

Method sentinelTimer at line 5098 of f-stack-2/sentinel.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	5111	5111
Object	rand	rand

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelTimer(void) {

```
....
5111.      server.hz = CONFIG_DEFAULT_HZ + rand() % CONFIG_DEFAULT_HZ;
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=678
Status	New

Method *sentinelVoteLeader at line 4378 of f-stack-2/sentinel.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	4398	4398
Object	rand	rand

Code Snippet
File Name f-stack-2/sentinel.c
Method char *sentinelVoteLeader(sentinelRedisInstance *master, uint64_t req_epoch, char *req_runid, uint64_t *leader_epoch) {

```
....
4398.              master->failover_start_time =
mstime()+rand()%SENTINEL_MAX_DESYNC;
```

Use of Insufficiently Random Values\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=679
Status	New

Method sentinelStartFailover at line 4577 of f-stack-2/sentinel.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	4586	4586
Object	rand	rand

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelStartFailover(sentinelRedisInstance *master) {

```
....
4586.       master->failover_start_time =
mstime()+rand()%SENTINEL_MAX_DESYNC;
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=680
Status	New

Method randn at line 1396 of f-stack-2/test_bbdev_perf.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	1401	1401
Object	rand	rand

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method randn(int n)

```
....
1401.             U1 = (double)rand() / RAND_MAX;
```

Use of Insufficiently Random Values\Path 11:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=681
Status	New

Method randn at line 1396 of f-stack-2/test_bbdev_perf.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/test_bbdev_perf.c	f-stack-2/test_bbdev_perf.c
Line	1402	1402
Object	rand	rand

Code Snippet
File Name f-stack-2/test_bbdev_perf.c
Method randn(int n)

```
....
1402.             U2 = (double)rand() / RAND_MAX;
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=682
Status	New

Method stringmatchlen_fuzz_test at line 173 of f-stack-2/util.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	179	179
Object	rand	rand

Code Snippet
File Name f-stack-2/util.c
Method int stringmatchlen_fuzz_test(void) {

```
....
179.          int strlen = rand() % sizeof(str);
```

Use of Insufficiently Random Values\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=683
Status	New

Method stringmatchlen_fuzz_test at line 173 of f-stack-2/util.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	180	180
Object	rand	rand

Code Snippet
File Name f-stack-2/util.c
Method int stringmatchlen_fuzz_test(void) {

```
....
180.          int patlen = rand() % sizeof(pat);
```

Use of Insufficiently Random Values\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=684
Status	New

Method stringmatchlen_fuzz_test at line 173 of f-stack-2/util.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	181	181
Object	rand	rand

Code Snippet
File Name f-stack-2/util.c
Method int stringmatchlen_fuzz_test(void) {

```
....
181.          for (int j = 0; j < strlen; j++) str[j] = rand() % 128;
```

Use of Insufficiently Random Values\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=685
Status	New

Method stringmatchlen_fuzz_test at line 173 of f-stack-2/util.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	182	182
Object	rand	rand

Code Snippet
File Name f-stack-2/util.c
Method int stringmatchlen_fuzz_test(void) {

```
....
182.          for (int j = 0; j < patlen; j++) pat[j] = rand() % 128;
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=27
Status	New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1515	1515
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1515.      for (bin = 0; bin <= max_index; bin++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=28
Status	New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1539	1539
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1539.       for (bin = 0; bin <= max_index; bin++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=29
Status	New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1546	1546
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1546.       for (bin = 0; bin <= max_index; bin++) {
```

Potential Off by One Error in Loops\Path 4:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=30
Status	New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1551	1551
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1551.       for (bin = 0; bin <= 3; bin++) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=31
Status	New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1563	1563
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1563.       for (bin = 0; bin <= max_index; bin++) {
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=32
Status	New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1589	1589
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1589.       for (bin = 0; bin <= half_hi; bin++) {
```

Potential Off by One Error in Loops\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=33
Status New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1617	1617
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1617.       for (bin = 0; bin <= half_hi; bin++) {
```

Potential Off by One Error in Loops\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=34
Status New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1637	1637
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1637.       for (bin = 0; bin <= half_hi; bin++) {
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=35
Status	New

The buffer allocated by <= in f-stack-2/ar9300_paprd.c at line 1385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/ar9300_paprd.c	f-stack-2/ar9300_paprd.c
Line	1709	1709
Object	<=	<=

Code Snippet
File Name f-stack-2/ar9300_paprd.c
Method HAL_BOOL create_pa_curve(u_int32_t * paprd_train_data_l,

```
....
1709.       for (bin = 0; bin <= half_hi; bin++) {
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=36
Status	New

The buffer allocated by <= in f-stack-2/vhost.c at line 611 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	f-stack-2/vhost.c	f-stack-2/vhost.c

Line	617	617
Object	<=	<=

Code Snippet
File Name f-stack-2/vhost.c
Method alloc_vring_queue(struct virtio_net *dev, uint32_t vring_idx)

```
....
617.        for (i = 0; i <= vring_idx; i++) {
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=981
Status	New

The loadAppendOnlyFile method in f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	755	755
Object	fopen	fopen

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
755.      FILE *fp = fopen(filename,"r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=982
Status	New

The rewriteAppendOnlyFile method in f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1555	1555
Object	fopen	fopen

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteAppendOnlyFile(char *filename) {

```
....
1555.       fp = fopen(tmpfile,"w");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=983
Status	New

The tlsConfigure method in f-stack-2/tls.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	f-stack-2/tls.c	f-stack-2/tls.c
Line	332	332
Object	fopen	fopen

Code Snippet
File Name f-stack-2/tls.c
Method int tlsConfigure(redisTLSContextConfig *ctx_config) {

```
....
332.           FILE *dhfile = fopen(ctx_config->dh_params_file, "r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=984
Status	New

The getRandomBytes method in f-stack-2/util.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	f-stack-2/util.c	f-stack-2/util.c
Line	658	658

Object	fopen	fopen

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.          FILE *fp = fopen("/dev/urandom","r");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=985
Status	New

The backgroundRewriteDoneHandler method in f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1866	1866
Object	open	open

Code Snippet
File Name f-stack-2/aof.c
Method void backgroundRewriteDoneHandler(int exitcode, int bysignal) {

```
....
1866.          newfd = open(tmpfile,O_WRONLY|O_APPEND);
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=986
Status	New

The backgroundRewriteDoneHandler method in f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	1932	1932

Object	open	open

Code Snippet
File Name f-stack-2/aof.c
Method void backgroundRewriteDoneHandler(int exitcode, int bysignal) {

```
....
1932.               oldfd =
open(server.aof_filename,O_RDONLY|O_NONBLOCK);
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=987
Status	New

The startAppendOnly method in f-stack-2/aof.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	f-stack-2/aof.c	f-stack-2/aof.c
Line	262	262
Object	open	open

Code Snippet
File Name f-stack-2/aof.c
Method int startAppendOnly(void) {

```
....
262.      newfd =
open(server.aof_filename,O_WRONLY|O_APPEND|O_CREAT,0644);
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=988
Status	New

The sentinelFlushConfig method in f-stack-2/sentinel.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	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	2317	2317
Object	open	open

Code Snippet	
File Name	f-stack-2/sentinel.c
Method	void sentinelFlushConfig(void) {

```
....
2317.       if ((fd = open(server.configfile,O_RDONLY)) == -1) goto werr;
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=952
Status	New

	Source	Destination
File	f-stack-2/bcmfs_qp.c	f-stack-2/bcmfs_qp.c
Line	381	381
Object	stats	sizeof

Code Snippet	
File Name	f-stack-2/bcmfs_qp.c
Method	void bcmfs_qp_stats_reset(struct bcmfs_qp **qp, int num_qp)

```
....
381.                memset(&qp[i]->stats, 0, sizeof(qp[i]->stats));
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=953
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	558	558
Object	buf	sizeof

Code Snippet	
File Name	f-stack-2/aof.c
Method	sds catAppendOnlyGenericCommand(sds dst, int argc, robj **argv) {

```
....
558.      len = 1+ll2string(buf+1,sizeof(buf)-1,argc);
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=954
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	723	723
Object	msg	sizeof

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
723.          vsnprintf(msg+strlen(msg), sizeof(msg)-strlen(msg), fmt,
ap);
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=955
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	706	706
Object	msg	sizeof

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
706.              snprintf(msg, sizeof(msg), "%s %s %s %d @ %s %s %d",
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=956
Status	New

	Source	Destination
File	f-stack-2/sentinel.c	f-stack-2/sentinel.c
Line	711	711
Object	msg	sizeof

Code Snippet
File Name f-stack-2/sentinel.c
Method void sentinelEvent(int level, char *type, sentinelRedisInstance *ri,

```
....
711.              snprintf(msg, sizeof(msg), "%s %s %s %d",
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=957
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	566	566
Object	buf	sizeof

Code Snippet
File Name f-stack-2/aof.c
Method sds catAppendOnlyGenericCommand(sds dst, int argc, robj **argv) {

```
....
566.          len = 1+ll2string(buf+1,sizeof(buf)-1,sdslen(o->ptr));
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=667
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	1555	1555
Object	fp	fp

Code Snippet
File Name f-stack-2/aof.c
Method int rewriteAppendOnlyFile(char *filename) {

```
....
1555.       fp = fopen(tmpfile,"w");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=668
Status	New

	Source	Destination
File	f-stack-2/aof.c	f-stack-2/aof.c
Line	755	755
Object	fp	fp

Code Snippet
File Name f-stack-2/aof.c
Method int loadAppendOnlyFile(char *filename) {

```
....
755.       FILE *fp = fopen(filename,"r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=669
Status	New

	Source	Destination
File	f-stack-2/tls.c	f-stack-2/tls.c

Line	332	332
Object	dhfile	dhfile

Code Snippet
File Name f-stack-2/tls.c
Method int tlsConfigure(redisTLSContextConfig *ctx_config) {

```
....
332.          FILE *dhfile = fopen(ctx_config->dh_params_file, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=670
Status New

	Source	Destination
File	f-stack-2/util.c	f-stack-2/util.c
Line	658	658
Object	fp	fp

Code Snippet
File Name f-stack-2/util.c
Method void getRandomBytes(unsigned char *p, size_t len) {

```
....
658.          FILE *fp = fopen("/dev/urandom","r");
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=777
Status New

	Source	Destination
File	f-stack-2/tls.c	f-stack-2/tls.c

Line	116	116
Object	mt	mt

Code Snippet
File Name f-stack-2/tls.c
Method static void sslLockingCallback(int mode, int lock_id, const char *f, int line) {

```
....
116.          pthread_mutex_lock(mt);
```

Unreleased Resource Leak\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=778
Status New

	Source	Destination
File	f-stack-2/tls.c	f-stack-2/tls.c
Line	134	134
Object	openssl_locks	openssl_locks

Code Snippet
File Name f-stack-2/tls.c
Method static void initCryptoLocks(void) {

```
....
134.          pthread_mutex_init(openssl_locks + i, NULL);
```

Unreleased Resource Leak\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=779
Status New

	Source	Destination
File	f-stack-2/tls.c	f-stack-2/tls.c
Line	134	134
Object	i	i

Code Snippet
File Name f-stack-2/tls.c
Method static void initCryptoLocks(void) {

```
....
134.          pthread_mutex_init(openssl_locks + i, NULL);
```

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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=179
Status	New

	Source	Destination
File	f-stack-2/bitops.c	f-stack-2/bitops.c
Line	1010	1010
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name f-stack-2/bitops.c
Method void bitfieldGeneric(client *c, int flags) {

```
....
1010.          j += 3 - (opcode == BITFIELDOP_GET);
```

Information Exposure Through Comments

Query Path:
CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description

Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030041&projectid=30036&pathid=989
Status	New

	Source	Destination

File	f-stack-2/test_cryptodev_blockcipher.c	f-stack-2/test_cryptodev_blockcipher.c
Line	706	706
Object	cipher-	cipher-

Code Snippet
File Name f-stack-2/test_cryptodev_blockcipher.c
Method /* cipher-only */

```
....
706.                    /* cipher-only */
```

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;
}
```

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

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;
```

```
  void setPassword()
 {
      password = System.console().readLine("Enter your password: ");
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}
```

```
int main()
{
    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n'){
                  password[i]='\0';
                  break;
            } else{
                  password[i++]=ch;
                  fflush(0);
            }
      }
      i=0;
      memset(password,'\0',256);
}

int main()
{
      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n')
                  break;
      }
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use After Free

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
//..
```

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));
    }
}
```

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
```

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 Dereference	**Development Concepts**

				(primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

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

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

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

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)
    }
```

```
}
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

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--;
           }
        }
    }
```

Information Leak Through Comments

Weakness ID: 615 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

- Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

Reference	Description
CVE-2007-6197	Version numbers and internal hostnames leaked in HTML comments.
CVE-2007-4072	CMS places full pathname of server in HTML comment.
CVE-2009-2431	blog software leaks real username in HTML comment.

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	**Development Concepts (primary)699 Research Concepts (primary)1000**

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	Anonymous Tool Vendor (under NDA)		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal

	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	6/19/2024
Common	0105849645654507	6/19/2024