freebsd-src-3 Scan Report

Project Name	freebsd-src-3
Scan Start	Saturday, June 22, 2024 2:04:22 AM
Preset	Checkmarx Default
Scan Time	03h:47m:04s
Lines Of Code Scanned	297677
Files Scanned	167
Report Creation Time	Saturday, June 22, 2024 9:05:46 AM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	6/1000 (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

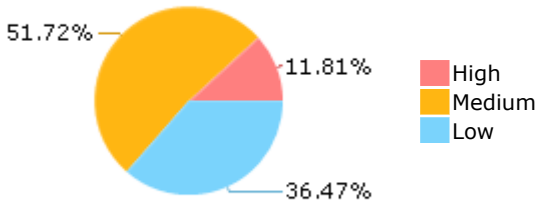
Results Limit

Results limit per query was set to 50

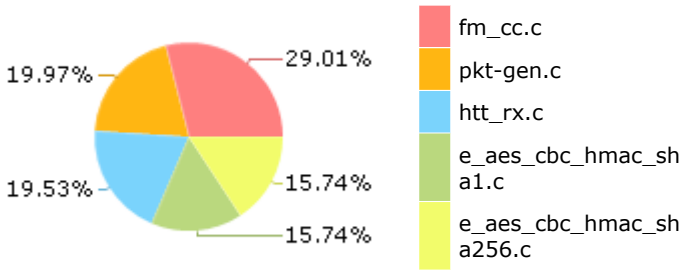
Selected Queries

Selected queries are listed in Result Summary

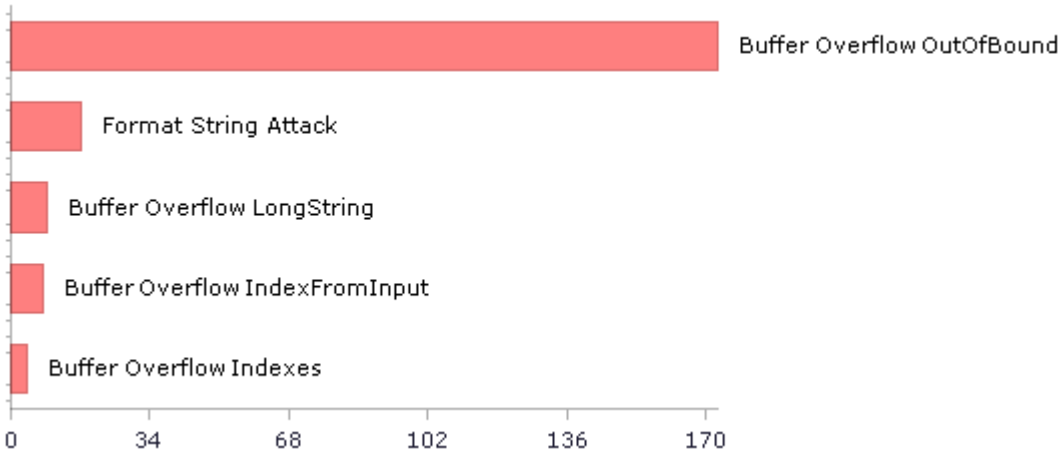
Result Summary



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	580	317
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	118	118
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	16	15
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	1	1
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	398	398
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	1	1
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	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	398	398
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	21	21
PCI DSS (3.2) - 6.5.2 - Buffer overflows	466	294
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.	6	6
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.	9	8
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.	154	133
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.	14	14
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.	28	28

***** 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)	125	125
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)	1	1
SC-13 Cryptographic Protection (P1)	4	3
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	34	13
SC-28 Protection of Information at Rest (P1)	17	17
SC-4 Information in Shared Resources (P1)	3	3
SC-5 Denial of Service Protection (P1)*	350	141
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	368	200
SI-11 Error Handling (P2)*	133	133
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	30	24

***** 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

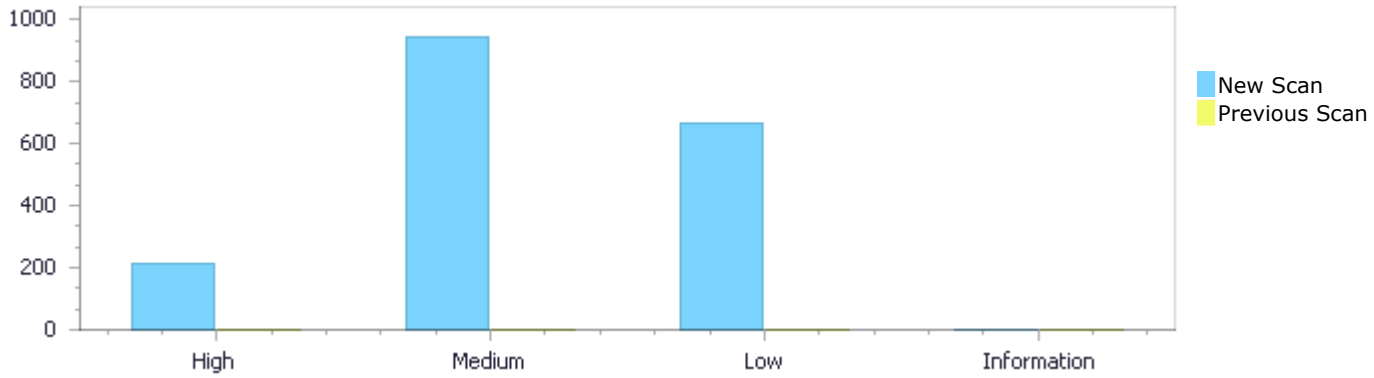
Scan Summary - Custom

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	216	946	667	0	1,829
Recurrent Issues	0	0	0	0	0
Total	216	946	667	0	1,829
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	216	946	667	0	1,829
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	216	946	667	0	1,829

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow OutOfBound	173	High
Format String Attack	17	High
Buffer Overflow LongString	9	High
Buffer Overflow IndexFromInput	8	High
Buffer Overflow Indexes	4	High

Buffer Overflow StrcpyStrcat	4	High
Buffer Overflow boundedcpy	1	High
Dangerous Functions	356	Medium
Buffer Overflow boundcpy WrongSizeParam	221	Medium
Use of Zero Initialized Pointer	150	Medium
Memory Leak	76	Medium
MemoryFree on StackVariable	37	Medium
Divide By Zero	31	Medium
Integer Overflow	27	Medium
Wrong Size t Allocation	16	Medium
Use of Uninitialized Pointer	10	Medium
Buffer Overflow Loops	6	Medium
Char Overflow	3	Medium
Double Free	3	Medium
Heap Inspection	2	Medium
Inadequate Encryption Strength	2	Medium
Use of a One Way Hash without a Salt	2	Medium
Wrong Memory Allocation	2	Medium
Short Overflow	1	Medium
Use of Hard coded Cryptographic Key	1	Medium
Unchecked Return Value	133	Low
Unchecked Array Index	124	Low
NULL Pointer Dereference	113	Low
Improper Resource Access Authorization	112	Low
Use of Obsolete Functions	42	Low
Reliance on DNS Lookups in a Decision	34	Low
Potential Off by One Error in Loops	21	Low
Sizeof Pointer Argument	18	Low
TOCTOU	16	Low
Use of Insufficiently Random Values	10	Low
Use of Sizeof On a Pointer Type	10	Low
Inconsistent Implementations	8	Low
Exposure of System Data to Unauthorized Control Sphere	7	Low
Information Exposure Through Comments	7	Low
Incorrect Permission Assignment For Critical Resources	6	Low
Potential Precision Problem	3	Low
Arithmenic Operation On Boolean	1	Low
Insecure Temporary File	1	Low
Potential Path Traversal	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
freebsd-src-3/fm_cc.c	174
freebsd-src-3/e_aes_cbc_hmac_sha1.c	107
freebsd-src-3/e_aes_cbc_hmac_sha256.c	107
freebsd-src-3/pkt-gen.c	91
freebsd-src-3/irdma_cm.c	59
freebsd-src-3/nfsd.c	54

freebsd-src-3/addrtoname.c	44
freebsd-src-3/if_bwn_phy_g.c	38
freebsd-src-3/init_sec_context.c	36
freebsd-src-3/htt_rx.c	31

Scan Results Details

Buffer Overflow OutOfBound

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

Categories

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

Description

Buffer Overflow OutOfBound\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=44
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in out, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	202
Object	ciph_d	out

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
202.          ciph_d[i].out = ciph_d[i - 1].out + packlen;
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=45
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in inp, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	201
Object	ciph_d	inp

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
201.          ciph_d[i].inp = hash_d[i].ptr = hash_d[i - 1].ptr + frag;
```

Buffer Overflow OutOfBound\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=46
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	203
Object	ciph_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
203.          memcpy(ciph_d[i].out - 16, IVs, 16);
```

Buffer Overflow OutOfBound\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=47
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	204
Object	ciph_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
204.          memcpy(ciph_d[i].iv, IVs, 16);
```

Buffer Overflow OutOfBound\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=48
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	264
Object	ciph_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
264.              ciph_d[i].blocks = MAXCHUNKSIZE / 16;
```

Buffer Overflow OutOfBound\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=600

	89&pathid=49
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in inp, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	274
Object	ciph_d	inp

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
274.                  ciph_d[i].inp += MAXCHUNKSIZE;
```

Buffer Overflow OutOfBound\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=50
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in out, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	275
Object	ciph_d	out

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
275.                  ciph_d[i].out += MAXCHUNKSIZE;
```

Buffer Overflow OutOfBound\Path 8:

Severity	High

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=51
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	276
Object	ciph_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
276.                  ciph_d[i].blocks = MAXCHUNKSIZE / 16;
```

Buffer Overflow OutOfBound\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=52
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	277
Object	ciph_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
277.                  memcpy(ciph_d[i].iv, ciph_d[i].out - 16, 16);
```

Buffer Overflow OutOfBound\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=53
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	277
Object	ciph_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
277.                  memcpy(ciph_d[i].iv, ciph_d[i].out - 16, 16);
```

Buffer Overflow OutOfBound\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=54
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	359
Object	ciph_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
359.          memcpy(ciph_d[i].out, ciph_d[i].inp, len - processed);
```

Buffer Overflow OutOfBound\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=55
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	359
Object	ciph_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
359.          memcpy(ciph_d[i].out, ciph_d[i].inp, len - processed);
```

Buffer Overflow OutOfBound\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=56
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in inp, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	360
Object	ciph_d	inp

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
360.          ciph_d[i].inp = ciph_d[i].out;
```

Buffer Overflow OutOfBound\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=57
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	360
Object	ciph_d	i

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
360.          ciph_d[i].inp = ciph_d[i].out;
```

Buffer Overflow OutOfBound\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=58
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	160	379

Object	ciph_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
160.      CIPH_DESC ciph_d[8];
....
379.          ciph_d[i].blocks = (len - processed) / 16;
```

Buffer Overflow OutOfBound\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=59
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	240
Object	hash_d	hash_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
240.          memcpy(blocks[i].c + 13, hash_d[i].ptr, 64 - 13);
```

Buffer Overflow OutOfBound\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=60
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ptr, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	201
Object	hash_d	ptr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
201.          ciph_d[i].inp = hash_d[i].ptr = hash_d[i - 1].ptr + frag;
```

Buffer Overflow OutOfBound\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=61
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ptr, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	241
Object	hash_d	ptr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
241.          hash_d[i].ptr += 64 - 13;
```

Buffer Overflow OutOfBound\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=62
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	242
Object	hash_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
242.          hash_d[i].blocks = (len - (64 - 13)) / 64;
```

Buffer Overflow OutOfBound\Path 20:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=63
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	262
Object	hash_d	i

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
262.              edges[i].ptr = hash_d[i].ptr;
```

Buffer Overflow OutOfBound\Path 21:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=64
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in ptr, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	271
Object	hash_d	ptr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
271.                  edges[i].ptr = hash_d[i].ptr += MAXCHUNKSIZE;
```

Buffer Overflow OutOfBound\Path 22:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=65
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	272
Object	hash_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
272.                  hash_d[i].blocks -= MAXCHUNKSIZE / 64;
```

Buffer Overflow OutOfBound\Path 23:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=66
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	290
Object	hash_d	i

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
290.              off = hash_d[i].blocks * 64;
```

Buffer Overflow OutOfBound\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=67
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	291
Object	hash_d	i

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
291.          const unsigned char *ptr = hash_d[i].ptr + off;
```

Buffer Overflow OutOfBound\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=68
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in q, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	226
Object	hash_d	q

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
226.          blocks[i].q[0] = BSWAP8(seqnum + i);
```

Buffer Overflow OutOfBound\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=69
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	233
Object	hash_d	c

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
233.          blocks[i].c[8] = ((u8 *)key->md.data)[8];
```

Buffer Overflow OutOfBound\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=70
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	234
Object	hash_d	c

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
234.          blocks[i].c[9] = ((u8 *)key->md.data)[9];
```

Buffer Overflow OutOfBound\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=71
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	235
Object	hash_d	c

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
235.          blocks[i].c[10] = ((u8 *)key->md.data)[10];
```

Buffer Overflow OutOfBound\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=72
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	237
Object	hash_d	c

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
237.          blocks[i].c[11] = (u8)(len >> 8);
```

Buffer Overflow OutOfBound\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=73
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	238

Object	hash_d	c

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
238.          blocks[i].c[12] = (u8)(len);
```

Buffer Overflow OutOfBound\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=74
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	240
Object	hash_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
240.          memcpy(blocks[i].c + 13, hash_d[i].ptr, 64 - 13);
```

Buffer Overflow OutOfBound\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=75
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	244
Object	hash_d	i

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
244.          edges[i].ptr = blocks[i].c;
```

Buffer Overflow OutOfBound\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=76
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	294
Object	hash_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
294.          memcpy(blocks[i].c, ptr, off);
```

Buffer Overflow OutOfBound\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=77
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	295
Object	hash_d	c

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
295.          blocks[i].c[off] = 0x80;
```

Buffer Overflow OutOfBound\Path 35:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=78
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	300
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
300.              blocks[i].d[15] = BSWAP4(len);
```

Buffer Overflow OutOfBound\Path 36:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=79
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	307
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
307.              blocks[i].d[31] = BSWAP4(len);
```

Buffer Overflow OutOfBound\Path 37:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=80
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	313
Object	hash_d	i

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
313.          edges[i].ptr = blocks[i].c;
```

Buffer Overflow OutOfBound\Path 38:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=81
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	322
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
322.          blocks[i].d[0] = BSWAP4(ctx->A[i]);
```

Buffer Overflow OutOfBound\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=82
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	324
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
324.          blocks[i].d[1] = BSWAP4(ctx->B[i]);
```

Buffer Overflow OutOfBound\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=83
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	326
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
326.          blocks[i].d[2] = BSWAP4(ctx->C[i]);
```

Buffer Overflow OutOfBound\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=84
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	328
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
328.          blocks[i].d[3] = BSWAP4(ctx->D[i]);
```

Buffer Overflow OutOfBound\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=85
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	330
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
330.          blocks[i].d[4] = BSWAP4(ctx->E[i]);
```

Buffer Overflow OutOfBound\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=86
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	332
Object	hash_d	c

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
332.          blocks[i].c[20] = 0x80;
```

Buffer Overflow OutOfBound\Path 44:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=87
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	333
Object	hash_d	d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
333.          blocks[i].d[15] = BSWAP4((64 + 20) * 8);
```

Buffer Overflow OutOfBound\Path 45:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=88
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	348

Object	hash_d	i

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
348.          edges[i].ptr = blocks[i].c;
```

Buffer Overflow OutOfBound\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=89
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in inp, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	201
Object	hash_d	inp

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
201.          ciph_d[i].inp = hash_d[i].ptr = hash_d[i - 1].ptr + frag;
```

Buffer Overflow OutOfBound\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=90
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in out, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	202
Object	hash_d	out

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
202.          ciph_d[i].out = ciph_d[i - 1].out + packlen;
```

Buffer Overflow OutOfBound\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=91
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	203
Object	hash_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
203.          memcpy(ciph_d[i].out - 16, IVs, 16);
```

Buffer Overflow OutOfBound\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=92
Status	New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	204
Object	hash_d	ciph_d

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
204.          memcpy(ciph_d[i].iv, IVs, 16);
```

Buffer Overflow OutOfBound\Path 50:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=93
Status New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	159	264
Object	hash_d	blocks

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
159.      HASH_DESC hash_d[8], edges[8];
....
264.              ciph_d[i].blocks = MAXCHUNKSIZE / 16;
```

Format String Attack

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

Categories

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

Description

Format String Attack\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=23
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "Can't open %s: %m\n" value from user input. This value is then used to construct a "format string" "Can't open %s: %m\n", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	462	462
Object	"Can't open %s: %m\n"	"Can't open %s: %m\n"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
462.              syslog(LOG_ERR, "Can't open %s: %m\n",
NFSD_STABLERESTART);
```

Format String Attack\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=24
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "Can't read stable storage file: %m\n" value from user input. This value is then used to construct a "format string" "Can't read stable storage file: %m\n", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	482	482
Object	"Can't read stable storage file: %m\n"	"Can't read stable storage file: %m\n"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
482.                    syslog(LOG_ERR, "Can't read stable storage file:
%m\n");
```

Format String Attack\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=25
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "fork: %m" value from user input. This value is then used to construct a "format string" "fork: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	497	497
Object	"fork: %m"	"fork: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
497.                    syslog(LOG_ERR, "fork: %m");
```

Format String Attack\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=26
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "can't bind udp addr %s: %m" value from user input. This value is then used to construct a "format string" "can't bind udp addr %s: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	535	535
Object	"can't bind udp addr %s: %m"	"can't bind udp addr %s: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
535.                                    "can't bind udp addr %s: %m",
```

Format String Attack\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=27
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "can't bind udp6 addr %s: %m" value from user input. This value is then used to construct a "format string" "can't bind udp6 addr %s: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	608	608
Object	"can't bind udp6 addr %s: %m"	"can't bind udp6 addr %s: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
608.                                    "can't bind udp6 addr %s: %m",
```

Format String Attack\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=28
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "setsockopt SO_REUSEADDR: %m" value from user input. This value is then used to construct a "format string" "setsockopt SO_REUSEADDR: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	677	677
Object	"setsockopt SO_REUSEADDR: %m"	"setsockopt SO_REUSEADDR: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
677.                                    "setsockopt SO_REUSEADDR: %m");
```

Format String Attack\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=29
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "can't bind tcp addr %s: %m" value from user input. This value is then used to construct a "format string" "can't bind tcp addr %s: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	681	681
Object	"can't bind tcp addr %s: %m"	"can't bind tcp addr %s: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
681.                                "can't bind tcp addr %s: %m",
```

Format String Attack\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=30
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "setsockopt SO_REUSEADDR: %m" value from user input. This value is then used to construct a "format string" "setsockopt SO_REUSEADDR: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	748	748
Object	"setsockopt SO_REUSEADDR: %m"	"setsockopt SO_REUSEADDR: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
748.                                    "setsockopt SO_REUSEADDR: %m");
```

Format String Attack\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=31
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "can't bind tcp6 addr %s: %m" value from user input. This value is then used to construct a "format string" "can't bind tcp6 addr %s: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	759	759
Object	"can't bind tcp6 addr %s: %m"	"can't bind tcp6 addr %s: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
759.                                    "can't bind tcp6 addr %s: %m",
```

Format String Attack\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=32
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "rpcb_set() failed, nothing to do: %m" value from user input. This value is then used to construct a "format string" "rpcb_set() failed, nothing to do: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	804	804
Object	"rpcb_set() failed, nothing to do: %m"	"rpcb_set() failed, nothing to do: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
804.                syslog(LOG_ERR, "rpcb_set() failed, nothing to do:
%m");
```

Format String Attack\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=33
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "tcp connects == 0, nothing to do: %m" value from user input. This value is then used to construct a "format string" "tcp connects == 0, nothing to do: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	809	809
Object	"tcp connects == 0, nothing to do: %m"	"tcp connects == 0, nothing to do: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
809.                syslog(LOG_ERR, "tcp connects == 0, nothing to do:
%m");
```

Format String Attack\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=34
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "select failed: %m" value from user input. This value is then used to construct a "format string" "select failed: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	836	836
Object	"select failed: %m"	"select failed: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
836.                            syslog(LOG_ERR, "select failed: %m");
```

Format String Attack\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=35
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "accept failed: %m" value from user input. This value is then used to construct a "format string" "accept failed: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	846	846
Object	"accept failed: %m"	"accept failed: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
846.                                syslog(LOG_ERR, "accept failed:
%m");
```

Format String Attack\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=36
Status	New

Method main at line 158 of freebsd-src-3/nfsd.c receives the "setsockopt SO_KEEPALIVE: %m" value from user input. This value is then used to construct a "format string" "setsockopt SO_KEEPALIVE: %m", which is provided as an argument to a string formatting function in main method of freebsd-src-3/nfsd.c at line 158.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	855	855
Object	"setsockopt SO_KEEPALIVE: %m"	"setsockopt SO_KEEPALIVE: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
855.                                    "setsockopt SO_KEEPALIVE: %m");
```

Format String Attack\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=37
Status	New

Method start_server at line 1019 of freebsd-src-3/nfsd.c receives the "nfssvc: %m" value from user input. This value is then used to construct a "format string" "nfssvc: %m", which is provided as an argument to a string formatting function in start_server method of freebsd-src-3/nfsd.c at line 1019.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1075	1075
Object	"nfssvc: %m"	"nfssvc: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method start_server(int master, struct nfsd_nfsd_args *nfsdargp, const char *vhost)

```
....
1075.                    syslog(LOG_ERR, "nfssvc: %m");
```

Format String Attack\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=38
Status	New

Method copy_stable at line 1140 of freebsd-src-3/nfsd.c receives the "stable restart copy failure: %m" value from user input. This value is then used to construct a "format string" "stable restart copy failure: %m", which is provided as an argument to a string formatting function in copy_stable method of freebsd-src-3/nfsd.c at line 1140.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1161	1161
Object	"stable restart copy failure: %m"	"stable restart copy failure: %m"

Code Snippet
File Name freebsd-src-3/nfsd.c
Method copy_stable(int from_fd, int to_fd)

```
....
1161.            syslog(LOG_ERR, "stable restart copy failure: %m");
```

Format String Attack\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=39
Status	New

Method ttloop at line 55 of freebsd-src-3/utility.c receives the "ttloop: read: %m\n" value from user input. This value is then used to construct a "format string" "ttloop: read: %m\n", which is provided as an argument to a string formatting function in ttloop method of freebsd-src-3/utility.c at line 55.

	Source	Destination
File	freebsd-src-3/utility.c	freebsd-src-3/utility.c
Line	66	66
Object	"ttloop: read: %m\n"	"ttloop: read: %m\n"

Code Snippet
File Name freebsd-src-3/utility.c
Method ttloop(void)

```
....
66.   syslog(LOG_INFO, "ttloop:  read: %m\n");
```

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=14
Status	New

The size of the buffer used by hs20_web_browser in argv, at line 66 of freebsd-src-3/browser-wpadebug.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hs20_web_browser passes to "browser-wpadebug", at line 66 of freebsd-src-3/browser-wpadebug.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/browser-wpadebug.c	freebsd-src-3/browser-wpadebug.c
Line	102	102
Object	"browser-wpadebug"	argv

Code Snippet
File Name freebsd-src-3/browser-wpadebug.c
Method int hs20_web_browser(const char *url, int ignore_tls)

```
....
102.              argv[0] = "browser-wpadebug";
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=15
Status	New

The size of the buffer used by hs20_web_browser in argv, at line 66 of freebsd-src-3/browser-wpadebug.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hs20_web_browser passes to "android.action.MAIN", at line 66 of freebsd-src-3/browser-wpadebug.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/browser-wpadebug.c	freebsd-src-3/browser-wpadebug.c
Line	105	105
Object	"android.action.MAIN"	argv

Code Snippet
File Name freebsd-src-3/browser-wpadebug.c
Method int hs20_web_browser(const char *url, int ignore_tls)

```
....
105.              argv[3] = "android.action.MAIN";
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=16
Status	New

The size of the buffer used by hs20_web_browser in argv, at line 66 of freebsd-src-3/browser-wpadebug.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hs20_web_browser passes to "android.intent.category.LAUNCHER", at line 66 of freebsd-src-3/browser-wpadebug.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/browser-wpadebug.c	freebsd-src-3/browser-wpadebug.c
Line	107	107
Object	"android.intent.category.LAUNCHER"	argv

Code Snippet
File Name freebsd-src-3/browser-wpadebug.c
Method int hs20_web_browser(const char *url, int ignore_tls)

```
....
107.              argv[5] = "android.intent.category.LAUNCHER";
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=17
Status	New

The size of the buffer used by hs20_web_browser in argv, at line 66 of freebsd-src-3/browser-wpadebug.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hs20_web_browser passes to "w1.fi.wpadebug/.WpaWebViewActivity", at line 66 of freebsd-src-3/browser-wpadebug.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/browser-wpadebug.c	freebsd-src-3/browser-wpadebug.c
Line	109	109
Object	"w1.fi.wpadebug/.WpaWebViewActivity"	argv

Code Snippet
File Name freebsd-src-3/browser-wpadebug.c
Method int hs20_web_browser(const char *url, int ignore_tls)

```
....
109.              argv[7] = "w1.fi.wpadebug/.WpaWebViewActivity";
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=18
Status	New

The size of the buffer used by hs20_web_browser in argv, at line 66 of freebsd-src-3/browser-wpadebug.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hs20_web_browser passes to "w1.fi.wpadebug.UR ", at line 66 of freebsd-src-3/browser-wpadebug.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/browser-wpadebug.c	freebsd-src-3/browser-wpadebug.c
Line	111	111
Object	"w1.fi.wpadebug.UR "	argv

Code Snippet
File Name freebsd-src-3/browser-wpadebug.c
Method int hs20_web_browser(const char *url, int ignore_tls)

```
....
111.              argv[9] = "w1.fi.wpadebug.URL";
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=19
Status	New

The size of the buffer used by test_Name in data, at line 319 of freebsd-src-3/check-gen.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_Name passes to "Love", at line 319 of freebsd-src-3/check-gen.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/check-gen.c	freebsd-src-3/check-gen.c
Line	355	355
Object	"Love"	data

Code Snippet
File Name freebsd-src-3/check-gen.c
Method test_Name (void)

```
....
355.      atv1[0].value.u.printableString.data = "Love";
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=20
Status	New

The size of the buffer used by test_Name in data, at line 319 of freebsd-src-3/check-gen.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_Name passes to "STOCKHOLM", at line 319 of freebsd-src-3/check-gen.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/check-gen.c	freebsd-src-3/check-gen.c

Line	361	361
Object	"STOCKHOLM"	data

Code Snippet
File Name freebsd-src-3/check-gen.c
Method test_Name (void)

```
....
361.      atv1[1].value.u.printableString.data = "STOCKHOLM";
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=21
Status	New

The size of the buffer used by test_Name in data, at line 319 of freebsd-src-3/check-gen.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_Name passes to "STOCKHOLM", at line 319 of freebsd-src-3/check-gen.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/check-gen.c	freebsd-src-3/check-gen.c
Line	374	374
Object	"STOCKHOLM"	data

Code Snippet
File Name freebsd-src-3/check-gen.c
Method test_Name (void)

```
....
374.      atv2[0].value.u.printableString.data = "STOCKHOLM";
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=22
Status	New

The size of the buffer used by test_Name in data, at line 319 of freebsd-src-3/check-gen.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_Name passes to "Love", at line 319 of freebsd-src-3/check-gen.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/check-gen.c	freebsd-src-3/check-gen.c
Line	380	380

Object	"Love"	data

Code Snippet
File Name freebsd-src-3/check-gen.c
Method test_Name (void)

```
....
380.      atv2[1].value.u.printableString.data = "Love";
```

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=6
Status	New

The size of the buffer used by increment in end_parms, at line 86 of freebsd-src-3/test_tparm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 168 of freebsd-src-3/test_tparm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/test_tparm.c	freebsd-src-3/test_tparm.c
Line	168	95
Object	argv	end_parms

Code Snippet
File Name freebsd-src-3/test_tparm.c
Method main(int argc, char *argv[])

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

File Name freebsd-src-3/test_tparm.c
Method increment(int *all_parms, int *num_parms, int len_parms, int end_parms)

```
....
95.   if (all_parms[end_parms]++ >= num_parms[end_parms]) {
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=7
Status	New

The size of the buffer used by hxtool_hex in strcspn, at line 1521 of freebsd-src-3/hxtool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hxtool_hex passes to stdin, at line 1521 of freebsd-src-3/hxtool.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1528	1529
Object	stdin	strcspn

Code Snippet
File Name freebsd-src-3/hxtool.c
Method hxtool_hex(struct hex_options *opt, int argc, char **argv)

```
....
1528.       while(fgets(buf, sizeof(buf), stdin) != NULL) {
1529.           buf[strcspn(buf, "\r\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=8
Status	New

The size of the buffer used by hxtool_hex in strcspn, at line 1521 of freebsd-src-3/hxtool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hxtool_hex passes to buf, at line 1521 of freebsd-src-3/hxtool.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1528	1529
Object	buf	strcspn

Code Snippet
File Name freebsd-src-3/hxtool.c
Method hxtool_hex(struct hex_options *opt, int argc, char **argv)

```
....
1528.       while(fgets(buf, sizeof(buf), stdin) != NULL) {
1529.           buf[strcspn(buf, "\r\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=9
Status	New

The size of the buffer used by main in UnaryNegation, at line 168 of freebsd-src-3/test_tparm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to stdin, at line 168 of freebsd-src-3/test_tparm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/test_tparm.c	freebsd-src-3/test_tparm.c
Line	254	260
Object	stdin	UnaryNegation

Code Snippet
File Name freebsd-src-3/test_tparm.c
Method main(int argc, char *argv[])

```
....
254.            while (fgets(buffer, sizeof(buffer) - 1, stdin) != 0) {
....
260.              while (t != s && isspace(UChar(t[-1])))
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=10
Status	New

The size of the buffer used by main in UnaryNegation, at line 168 of freebsd-src-3/test_tparm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to buffer, at line 168 of freebsd-src-3/test_tparm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/test_tparm.c	freebsd-src-3/test_tparm.c
Line	254	260
Object	buffer	UnaryNegation

Code Snippet
File Name freebsd-src-3/test_tparm.c
Method main(int argc, char *argv[])

```
....
254.            while (fgets(buffer, sizeof(buffer) - 1, stdin) != 0) {
....
260.              while (t != s && isspace(UChar(t[-1])))
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=11
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1908 of freebsd-src-3/pkinit.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1908 of freebsd-src-3/pkinit.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1919	1922
Object	buf	strcspn

Code Snippet
File Name freebsd-src-3/pkinit.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1919.      while (fgets(buf, sizeof(buf), f) != NULL) {
....
1922.       buf[strcspn(buf, "\n")] = '\0';
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=12
Status	New

The size of the buffer used by zread in zs_code, at line 214 of freebsd-src-3/zuncompress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zread passes to BinaryExpr, at line 214 of freebsd-src-3/zuncompress.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/zuncompress.c	freebsd-src-3/zuncompress.c
Line	240	315
Object	BinaryExpr	zs_code

Code Snippet
File Name freebsd-src-3/zuncompress.c
Method zread(void *cookie, char *rbp, int num)

```
....
240.        if (fread(header + i, 1, sizeof(header) - i, zs->zs_fp) !=
....
315.                    tab_suffixof(zs->u.r.zs_code) = zs-
>u.r.zs_finchar;
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=13
Status	New

The size of the buffer used by zread in zs_code, at line 214 of freebsd-src-3/zuncompress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that zread passes to BinaryExpr, at line 214 of freebsd-src-3/zuncompress.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/zuncompress.c	freebsd-src-3/zuncompress.c
Line	240	314
Object	BinaryExpr	zs_code

Code Snippet
File Name freebsd-src-3/zuncompress.c
Method zread(void *cookie, char *rbp, int num)

```
....
240.        if (fread(header + i, 1, sizeof(header) - i, zs->zs_fp) !=
....
314.                    tab_prefixof(zs->u.r.zs_code) = (u_short) zs-
>u.r.zs_oldcode;
```

Buffer Overflow Indexes

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

Categories

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

Description
Buffer Overflow Indexes\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1
Status	New

The size of the buffer used by main in optind, at line 2066 of freebsd-src-3/hostapd_cli.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 2066 of freebsd-src-3/hostapd_cli.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	2066	2181
Object	argc	optind

Code Snippet	
File Name	freebsd-src-3/hostapd_cli.c
Method	int main(int argc, char *argv[])

```
....
2066.  int main(int argc, char *argv[])
....
2181.              wpa_request(ctrl_conn, argc - optind, &argv[optind]);
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=2
Status	New

The size of the buffer used by main in uri, at line 215 of freebsd-src-3/https-client.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 215 of freebsd-src-3/https-client.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	215	340
Object	argv	uri

Code Snippet	
File Name	freebsd-src-3/https-client.c
Method	main(int argc, char **argv)

```
....
215.  main(int argc, char **argv)
....
340.        uri[sizeof(uri) - 1] = '\0';
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=3
Status	New

The size of the buffer used by main in sizeof, at line 215 of freebsd-src-3/https-client.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 215 of freebsd-src-3/https-client.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	215	340

Object	argv	sizeof

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
215.  main(int argc, char **argv)
....
340.        uri[sizeof(uri) - 1] = '\0';
```

Buffer Overflow Indexes\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=4
Status New

The size of the buffer used by hxtool_hex in strcspn, at line 1521 of freebsd-src-3/hxtool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hxtool_hex passes to stdin, at line 1521 of freebsd-src-3/hxtool.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1528	1529
Object	stdin	strcspn

Code Snippet
File Name freebsd-src-3/hxtool.c
Method hxtool_hex(struct hex_options *opt, int argc, char **argv)

```
....
1528.       while(fgets(buf, sizeof(buf), stdin) != NULL) {
1529.           buf[strcspn(buf, "\r\n")] = '\0';
```

Buffer Overflow StrcpyStrcat

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=40

Status	New

The size of the buffer used by parse_dsserver in mdsp, at line 1179 of freebsd-src-3/nfsd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_dsserver passes to optionarg, at line 1179 of freebsd-src-3/nfsd.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1179	1269
Object	optionarg	mdsp

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1179.  parse_dsserver(const char *optionarg, struct nfsd_nfsd_args
*nfsdargp)
....
1269.                   strcpy(&mdspath[mdspathcnt], mdsp);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=41
Status	New

The size of the buffer used by parse_dsserver in Address, at line 1179 of freebsd-src-3/nfsd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_dsserver passes to optionarg, at line 1179 of freebsd-src-3/nfsd.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1179	1269
Object	optionarg	Address

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1179.  parse_dsserver(const char *optionarg, struct nfsd_nfsd_args
*nfsdargp)
....
1269.                   strcpy(&mdspath[mdspathcnt], mdsp);
```

Buffer Overflow StrcpyStrcat\Path 3:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=42
Status	New

The size of the buffer used by parse_dsserver in mdspath, at line 1179 of freebsd-src-3/nfsd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_dsserver passes to optionarg, at line 1179 of freebsd-src-3/nfsd.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1179	1269
Object	optionarg	mdspath

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1179.  parse_dsserver(const char *optionarg, struct nfsd_nfsd_args
*nfsdargp)
....
1269.                   strcpy(&mdspath[mdspathcnt], mdsp);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=43
Status	New

The size of the buffer used by tap_alloc in dev, at line 2861 of freebsd-src-3/pkt-gen.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tap_alloc passes to dev, at line 2861 of freebsd-src-3/pkt-gen.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	2861	2918
Object	dev	dev

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method tap_alloc(char *dev)

```
....
2861.  tap_alloc(char *dev)
....
2918.       strcpy(dev, ifr.ifr_name);
```

Buffer Overflow boundedcpy

Query Path:

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

Categories

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

Description

Buffer Overflow boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=5
Status	New

The size parameter sizeof in line 168 in file freebsd-src-3/test_tparm.c is influenced by the user input argv in line 168 in file freebsd-src-3/test_tparm.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	freebsd-src-3/test_tparm.c	freebsd-src-3/test_tparm.c
Line	168	344
Object	argv	sizeof

Code Snippet
File Name freebsd-src-3/test_tparm.c
Method main(int argc, char *argv[])

```
....
168.  main(int argc, char *argv[])
....
344.                  memset(all_parms, 0, sizeof(all_parms));
```

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=1060099&projectid=60089&pathid=559
Status	New

The dangerous function, _snprintf, was found in use at line 215 in freebsd-src-3/https-client.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	336	336
Object	_snprintf	_snprintf

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
336.              snprintf(uri, sizeof(uri) - 1, "%s", path);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=560
Status	New

The dangerous function, _snprintf, was found in use at line 215 in freebsd-src-3/https-client.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	338	338
Object	_snprintf	_snprintf

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
338.              snprintf(uri, sizeof(uri) - 1, "%s?%s", path, query);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=561
Status	New

The dangerous function, alloca, was found in use at line 88 in freebsd-src-3/ldns-host.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c

Line	93	93
Object	alloca	alloca

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_rdf_reverse_a(ldns_rdf *addr, const char *base) {

```
....
93.      buf = alloca(LDNS_IP4ADDRLEN*4 + len + 1);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=562
Status	New

The dangerous function, alloca, was found in use at line 102 in freebsd-src-3/ldns-host.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	107	107
Object	alloca	alloca

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_rdf_reverse_aaaa(ldns_rdf *addr, const char *base) {

```
....
107.      buf = alloca(LDNS_IP6ADDRLEN*4 + len + 1);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=563
Status	New

The dangerous function, alloca, was found in use at line 944 in freebsd-src-3/ldns-host.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	956	956
Object	alloca	alloca

Code Snippet	
File Name	freebsd-src-3/ldns-host.c
Method	dosoa(ldns_resolver *res, ldns_rdf *domain, bool absolute) {

```
....
956.      nsaddrs = alloca(cnt*sizeof(*nsaddrs));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=564
Status	New

The dangerous function, memcpy, was found in use at line 146 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	161	161
Object	memcpy	memcpy

Code Snippet	
File Name	freebsd-src-3/addrtoname.c
Method	win32_gethostbyaddr(const char *addr, int len, int type)

```
....
161.              memcpy(&addr6.sin6_addr, addr, len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=565
Status	New

The dangerous function, memcpy, was found in use at line 276 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	282	282
Object	memcpy	memcpy

Code Snippet	
File Name	freebsd-src-3/addrtoname.c

Method	ipaddr_string(netdissect_options *ndo, const u_char *ap)

```
....
282.        memcpy(&addr, ap, sizeof(addr));
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=566
Status	New

The dangerous function, memcpy, was found in use at line 335 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	349	349
Object	memcpy	memcpy

Code Snippet	
File Name	freebsd-src-3/addrtoname.c
Method	ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
349.        memcpy(&addr, ap, sizeof(addr));
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=567
Status	New

The dangerous function, memcpy, was found in use at line 335 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	355	355
Object	memcpy	memcpy

Code Snippet	
File Name	freebsd-src-3/addrtoname.c
Method	ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
355.        memcpy(p->addr, addr.addr, sizeof(nd_ipv6));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=568
Status	New

The dangerous function, memcpy, was found in use at line 467 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	504	504
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_bytestring(netdissect_options *ndo, const u_char *bs,

```
....
504.        memcpy(tp->bs_bytes, bs, nlen);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=569
Status	New

The dangerous function, memcpy, was found in use at line 517 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	551	551
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_nsap(netdissect_options *ndo, const u_char *nsap,

```
....
551.        memcpy((char *)&tp->e_nsap[1], (const char *)nsap,
nsap_length);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=570
Status	New

The dangerous function, memcpy, was found in use at line 588 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	609	609
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method etheraddr_string(netdissect_options *ndo, const uint8_t *ep)

```
....
609.              memcpy (&ea, ep, MAC_ADDR_LEN);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=571
Status	New

The dangerous function, memcpy, was found in use at line 896 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	909	909
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method init_protoidarray(netdissect_options *ndo)

```
....
909.              memcpy((char *)&protoid[3], (char *)&etype, 2);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=572
Status	New

The dangerous function, memcpy, was found in use at line 950 in freebsd-src-3/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	987	987
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method init_etherarray(netdissect_options *ndo)

```
....
987.              memcpy (&ea, el->addr, MAC_ADDR_LEN);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=573
Status	New

The dangerous function, memcpy, was found in use at line 62 in freebsd-src-3/bthidcontrol.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	68	68
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method main(int argc, char *argv[])

```
....
68.    memcpy(&bdaddr, NG_HCI_BDADDR_ANY, sizeof(bdaddr));
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=574
Status	New

The dangerous function, memcpy, was found in use at line 62 in freebsd-src-3/bthidcontrol.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	79	79
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method main(int argc, char *argv[])

```
....
79.                     memcpy(&bdaddr, he->h_addr, sizeof(bdaddr));
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=575
Status	New

The dangerous function, memcpy, was found in use at line 768 in freebsd-src-3/compile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	845	845
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_tr(char *p, struct s_tr **py)

```
....
845.                            memcpy(y->multis[i].from, op, oclen);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=576
Status	New

The dangerous function, memcpy, was found in use at line 768 in freebsd-src-3/compile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	847	847
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_tr(char *p, struct s_tr **py)

```
....
847.                            memcpy(y->multis[i].to, np, nclen);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=577
Status	New

The dangerous function, memcpy, was found in use at line 198 in freebsd-src-3/crypto-pk.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/crypto-pk.c	freebsd-src-3/crypto-pk.c
Line	284	284
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/crypto-pk.c
Method _krb5_pk_kdf(krb5_context context,

```
....
284.        memcpy((unsigned char *)keydata + offset,
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=578
Status	New

The dangerous function, memcpy, was found in use at line 39 in freebsd-src-3/crypto-pk.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/crypto-pk.c	freebsd-src-3/crypto-pk.c
Line	91	91
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/crypto-pk.c
Method _krb5_pk_octetstring2key(krb5_context context,

```
....
91.   memcpy((unsigned char *)keydata + offset,
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=579
Status	New

The dangerous function, memcpy, was found in use at line 222 in freebsd-src-3/digest.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/digest.c	freebsd-src-3/digest.c
Line	243	243
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/digest.c
Method int EVP_MD_CTX_copy_ex(EVP_MD_CTX *out, const EVP_MD_CTX *in)

```
....
243.      memcpy(out, in, sizeof(*out));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=580
Status	New

The dangerous function, memcpy, was found in use at line 222 in freebsd-src-3/digest.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/digest.c	freebsd-src-3/digest.c
Line	265	265
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/digest.c
Method int EVP_MD_CTX_copy_ex(EVP_MD_CTX *out, const EVP_MD_CTX *in)

```
....
265.          memcpy(out->md_data, in->md_data, out->digest->ctx_size);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=581
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	196	196
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
196.      memcpy(ciph_d[0].out - 16, IVs, 16);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=582
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	197	197
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
197.      memcpy(ciph_d[0].iv, IVs, 16);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=583
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	203	203
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
203.          memcpy(ciph_d[i].out - 16, IVs, 16);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=584
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	204	204
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
204.          memcpy(ciph_d[i].iv, IVs, 16);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=585
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	209	209
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
209.      memcpy(blocks[0].c, key->md.data, 8);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=586
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	240	240
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
240.          memcpy(blocks[i].c + 13, hash_d[i].ptr, 64 - 13);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=587
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	277	277
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
277.                    memcpy(ciph_d[i].iv, ciph_d[i].out - 16, 16);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=588
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	294	294
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
294.            memcpy(blocks[i].c, ptr, off);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=589
Status	New

The dangerous function, memcpy, was found in use at line 154 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	359	359
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
359.          memcpy(ciph_d[i].out, ciph_d[i].inp, len - processed);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=590
Status	New

The dangerous function, memcpy, was found in use at line 402 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	455	455
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
455.                    memcpy(out + aes_off, in + aes_off, plen -
aes_off);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=591
Status	New

The dangerous function, memcpy, was found in use at line 402 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	502	502
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
502.                    memcpy(EVP_CIPHER_CTX_iv_noconst(ctx), in,
AES_BLOCK_SIZE);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=592
Status	New

The dangerous function, memcpy, was found in use at line 402 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	513	513
Object	memcpy	memcpy

Code Snippet

File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c

Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
513.                    memcpy(tail_iv, in + len - 2 * AES_BLOCK_SIZE,
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=593
Status	New

The dangerous function, memcpy, was found in use at line 402 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	569	569
Object	memcpy	memcpy

Code Snippet

File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c

Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
569.                    memcpy(ctx->iv, tail_iv, AES_BLOCK_SIZE);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=594
Status	New

The dangerous function, memcpy, was found in use at line 768 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	786	786
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```
....
786.                    memcpy(hmac_key, ptr, arg);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=595
Status	New

The dangerous function, memcpy, was found in use at line 768 in freebsd-src-3/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	830	830
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```
....
830.                    memcpy(key->aux.tls_aad, ptr, arg);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=596
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	193	193
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
193.      memcpy(ciph_d[0].out - 16, IVs, 16);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=597
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	194	194
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
194.      memcpy(ciph_d[0].iv, IVs, 16);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=598
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	200	200
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
200.          memcpy(ciph_d[i].out - 16, IVs, 16);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=599
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	201	201
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
201.          memcpy(ciph_d[i].iv, IVs, 16);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=600
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	206	206
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
206.      memcpy(blocks[0].c, key->md.data, 8);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=601
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	240	240
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
240.          memcpy(blocks[i].c + 13, hash_d[i].ptr, 64 - 13);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=602
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	277	277
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
277.                  memcpy(ciph_d[i].iv, ciph_d[i].out - 16, 16);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=603
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	294	294
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
294.          memcpy(blocks[i].c, ptr, off);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=604
Status	New

The dangerous function, memcpy, was found in use at line 150 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	371	371
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
371.          memcpy(ciph_d[i].out, ciph_d[i].inp, len - processed);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=605
Status	New

The dangerous function, memcpy, was found in use at line 417 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	485	485
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
....
485.                    memcpy(out + aes_off, in + aes_off, plen -
aes_off);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=606
Status	New

The dangerous function, memcpy, was found in use at line 745 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	767	767
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```
....
767.                    memcpy(hmac_key, ptr, arg);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=607
Status	New

The dangerous function, memcpy, was found in use at line 745 in freebsd-src-3/e_aes_cbc_hmac_sha256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	811	811
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```
....
811.                    memcpy(key->aux.tls_aad, ptr, arg);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=608
Status	New

The dangerous function, memcpy, was found in use at line 15 in freebsd-src-3/es256.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freebsd-src-3/es256.c	freebsd-src-3/es256.c
Line	24	24
Object	memcpy	memcpy

Code Snippet
File Name freebsd-src-3/es256.c
Method decode_coord(const cbor_item_t *item, void *xy, size_t xy_len)

```
....
24.   memcpy(xy, cbor_bytestring_handle(item), xy_len);
```

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=1060099&projectid=60089&pathid=217
Status	New

The size of the buffer used by ip6addr_string in nd_ipv6, at line 335 of freebsd-src-3/addrtoname.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ip6addr_string passes to nd_ipv6, at line 335 of freebsd-src-3/addrtoname.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c

Line	355	355
Object	nd_ipv6	nd_ipv6

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
355.        memcpy(p->addr, addr.addr, sizeof(nd_ipv6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=218
Status	New

The size of the buffer used by es256_pk_set_x in ->, at line 187 of freebsd-src-3/es256.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that es256_pk_set_x passes to ->, at line 187 of freebsd-src-3/es256.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/es256.c	freebsd-src-3/es256.c
Line	189	189
Object	->	->

Code Snippet
File Name freebsd-src-3/es256.c
Method es256_pk_set_x(es256_pk_t *pk, const unsigned char *x)

```
....
189.        memcpy(pk->x, x, sizeof(pk->x));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=219
Status	New

The size of the buffer used by es256_pk_set_y in ->, at line 195 of freebsd-src-3/es256.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that es256_pk_set_y passes to ->, at line 195 of freebsd-src-3/es256.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/es256.c	freebsd-src-3/es256.c
Line	197	197

Object	->	->

Code Snippet
File Name freebsd-src-3/es256.c
Method es256_pk_set_y(es256_pk_t *pk, const unsigned char *y)

```
....
197.        memcpy(pk->y, y, sizeof(pk->y));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=220
Status	New

The size of the buffer used by BuildNewNodeAddOrMdfyKeyAndNextEngine in t_FmPcdCcNextEngineParams, at line 2566 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	2600	2600
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2600.              &p_KeyParams->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=1060099&projectid=60089&pathid=221
Status	New

The size of the buffer used by BuildNewNodeModifyNextEngine in t_FmPcdCcNextEngineParams, at line 3094 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	3125	3125
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

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

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=222
Status New

The size of the buffer used by ModifyNodeCommonPart in t_FmPcdCcKeyAndNextEngineParams, at line 3429 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3530	3530
Object	t_FmPcdCcKeyAndNextEngineParams	t_FmPcdCcKeyAndNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

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

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=223
Status New

The size of the buffer used by ModifyNodeCommonPart in t_FmPcdCcKeyAndNextEngineParams, at line 3429 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	3544	3544
Object	t_FmPcdCcKeyAndNextEngineParams	t_FmPcdCcKeyAndNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_FmPcdModifyCcKeyAdditionalParams * ModifyNodeCommonPart(

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

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=224
Status	New

The size of the buffer used by CheckParams in t_FmPcdCcNextEngineParams, at line 3705 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3739	3739
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/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 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=225
Status	New

The size of the buffer used by CheckParams in t_FmPcdCcNextEngineParams, at line 3705 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	3795	3795
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/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 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=226
Status New

The size of the buffer used by Ipv4TtlOrIpv6HopLimitCheckParams in t_FmPcdCcNextEngineParams, at line 3825 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3873	3873
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error Ipv4TtlOrIpv6HopLimitCheckParams(

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

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=227
Status New

The size of the buffer used by Ipv4TtlOrIpv6HopLimitCheckParams in t_FmPcdCcNextEngineParams, at line 3825 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	3926	3926
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error Ipv4TtlOrIpv6HopLimitCheckParams(

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

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=228
Status	New

The size of the buffer used by IcHashIndexedCheckParams in t_FmPcdCcNextEngineParams, at line 3946 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4036	4036
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error IcHashIndexedCheckParams(t_Handle h_FmPcd,

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

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=229
Status	New

The size of the buffer used by EnqueueNodeInfoToRelevantLst in t_CcNodeInformation, at line 4938 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	4950	4950
Object	t_CcNodeInformation	t_CcNodeInformation

Code Snippet
File Name freebsd-src-3/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 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=230
Status New

The size of the buffer used by FM_PCD_CcRootBuild in t_FmPcdCcNextEngineParams, at line 5994 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	6148	6148
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

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

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=231
Status New

The size of the buffer used by FM_PCD_CcRootBuild in t_FmPcdCcKeyAndNextEngineParams, at line 5994 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	6204	6204
Object	t_FmPcdCcKeyAndNextEngineParams	t_FmPcdCcKeyAndNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

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

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=232
Status	New

The size of the buffer used by FM_PCD_MatchTableGetNextEngine in t_FmPcdCcNextEngineParams, at line 6908 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	6929	6929
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Error FM_PCD_MatchTableGetNextEngine(

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

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=233
Status	New

The size of the buffer used by FM_PCD_HashTableGetMissNextEngine in t_FmPcdCcNextEngineParams, at line 7489 of freebsd-src-3/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 freebsd-src-3/fm_cc.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	7504	7504
Object	t_FmPcdCcNextEngineParams	t_FmPcdCcNextEngineParams

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Error FM_PCD_HashTableGetMissNextEngine(

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

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=234
Status	New

The size of the buffer used by freebsd32_ffclock_setestimate in uint64_t, at line 4025 of freebsd-src-3/freebsd32_misc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that freebsd32_ffclock_setestimate passes to uint64_t, at line 4025 of freebsd-src-3/freebsd32_misc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	4041	4041
Object	uint64_t	uint64_t

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_ffclock_setestimate(struct thread *td,

```
....
4041.       memcpy(&cest.update_time.frac, &cest32.update_time.frac,
sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=235
Status	New

The size of the buffer used by freebsd32_ffclock_getestimate in ffclock_estimate, at line 4059 of freebsd-src-3/freebsd32_misc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that freebsd32_ffclock_getestimate passes to ffclock_estimate, at line 4059 of freebsd-src-3/freebsd32_misc.c, to overwrite the target buffer.

	Source	Destination

File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	4067	4067
Object	ffclock_estimate	ffclock_estimate

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_ffclock_getestimate(struct thread *td,

```
....
4067.       memcpy(&cest, &ffclock_estimate, sizeof(struct
ffclock_estimate));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=236
Status	New

The size of the buffer used by freebsd32_ffclock_getestimate in uint64_t, at line 4059 of freebsd-src-3/freebsd32_misc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that freebsd32_ffclock_getestimate passes to uint64_t, at line 4059 of freebsd-src-3/freebsd32_misc.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	4071	4071
Object	uint64_t	uint64_t

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_ffclock_getestimate(struct thread *td,

```
....
4071.       memcpy(&cest32.update_time.frac, &cest.update_time.frac,
sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=237
Status	New

The size of the buffer used by iwl_mvm_ftm_responder_dyn_cfg_v3 in Namespace2058109273, at line 213 of freebsd-src-3/ftm-responder.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iwl_mvm_ftm_responder_dyn_cfg_v3 passes to Namespace2058109273, at line 213 of freebsd-src-3/ftm-responder.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/ftm-responder.c	freebsd-src-3/ftm-responder.c
Line	263	263
Object	Namespace2058109273	Namespace2058109273

Code Snippet
File Name freebsd-src-3/ftm-responder.c
Method iwl_mvm_ftm_responder_dyn_cfg_v3(struct iwl_mvm *mvm,

```
....
263.              memcpy(cmd.addr, hltk_data->addr, sizeof(cmd.addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=238
Status New

The size of the buffer used by iwl_mvm_ftm_responder_dyn_cfg_v3 in Namespace2058109273, at line 213 of freebsd-src-3/ftm-responder.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that iwl_mvm_ftm_responder_dyn_cfg_v3 passes to Namespace2058109273, at line 213 of freebsd-src-3/ftm-responder.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/ftm-responder.c	freebsd-src-3/ftm-responder.c
Line	264	264
Object	Namespace2058109273	Namespace2058109273

Code Snippet
File Name freebsd-src-3/ftm-responder.c
Method iwl_mvm_ftm_responder_dyn_cfg_v3(struct iwl_mvm *mvm,

```
....
264.              memcpy(cmd.hltk_buf, hltk_data->hltk,
sizeof(cmd.hltk_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=239
Status New

The size of the buffer used by ath10k_htt_rx_h_undecap_eth in rfc1042_hdr, at line 1719 of freebsd-src-3/htt_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath10k_htt_rx_h_undecap_eth passes to rfc1042_hdr, at line 1719 of freebsd-src-3/htt_rx.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	1769	1769
Object	rfc1042_hdr	rfc1042_hdr

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static void ath10k_htt_rx_h_undecap_eth(struct ath10k *ar,

```
....
1769.                sizeof(struct rfc1042_hdr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=240
Status	New

The size of the buffer used by ath10k_htt_t2h_msg_handler in Namespace906951118, at line 4212 of freebsd-src-3/htt_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath10k_htt_t2h_msg_handler passes to Namespace906951118, at line 4212 of freebsd-src-3/htt_rx.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	4252	4252
Object	Namespace906951118	Namespace906951118

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method bool ath10k_htt_t2h_msg_handler(struct ath10k *ar, struct sk_buff *skb)

```
....
4252.            memcpy(ev.addr, resp->peer_map.addr, sizeof(ev.addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=241
Status	New

The size of the buffer used by bwn_lo_probe_loctl in bwn_loctl, at line 2372 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_probe_loctl passes to bwn_loctl, at line 2372 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2401	2401
Object	bwn_loctl	bwn_loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_probe_loctl(struct bwn_mac *mac,

```
....
2401.       memcpy(&orig, probe, sizeof(struct bwn_loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=242
Status New

The size of the buffer used by bwn_lo_probe_loctl in bwn_loctl, at line 2372 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_probe_loctl passes to bwn_loctl, at line 2372 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2406	2406
Object	bwn_loctl	bwn_loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_probe_loctl(struct bwn_mac *mac,

```
....
2406.            memcpy(&test, &orig, sizeof(struct bwn_loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=243
Status New

The size of the buffer used by bwn_lo_probe_loctl in bwn_loctl, at line 2372 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_probe_loctl passes to bwn_loctl, at line 2372 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2416	2416
Object	bwn_loctl	bwn_loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_probe_loctl(struct bwn_mac *mac,

```
....
2416.                                sizeof(struct bwn_loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=244
Status New

The size of the buffer used by bwn_lo_probe_sm in bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_probe_sm passes to bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2451	2451
Object	bwn_loctl	bwn_loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_probe_sm(struct bwn_mac *mac, struct bwn_loctl *loctl, int *rxgain)

```
....
2451.       memcpy(&d.loctl, loctl, sizeof(struct bwn_loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=245
Status New

The size of the buffer used by bwn_lo_probe_sm in bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_probe_sm passes to bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2472	2472
Object	bwn_loctl	bwn_loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_probe_sm(struct bwn_mac *mac, struct bwn_loctl *loctl, int *rxgain)

```
....
2472.                           sizeof(struct bwn_loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=246
Status	New

The size of the buffer used by bwn_lo_probe_sm in bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_probe_sm passes to bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2478	2478
Object	bwn_loctl	bwn_loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_probe_sm(struct bwn_mac *mac, struct bwn_loctl *loctl, int *rxgain)

```
....
2478.                   memcpy(&d.loctl, &probe, sizeof(struct
bwn_loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=247
Status	New

The size of the buffer used by bwn_lo_probe_sm in bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_probe_sm passes to bwn_loctl, at line 2437 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2481	2481
Object	bwn_loctl	bwn_loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_probe_sm(struct bwn_mac *mac, struct bwn_loctl *loctl, int *rxgain)

```
....
2481.            memcpy(loctl, &d.loctl, sizeof(struct bwn_loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=248
Status	New

The size of the buffer used by bwn_lo_calibset in bbatt, at line 2502 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_calibset passes to bbatt, at line 2502 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2538	2538
Object	bbatt	bbatt

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_calibset(struct bwn_mac *mac,

```
....
2538.       memcpy(&cal->bbatt, bbatt, sizeof(*bbatt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=249
Status	New

The size of the buffer used by bwn_lo_calibset in rfatt, at line 2502 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_calibset passes to rfatt, at line 2502 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2539	2539
Object	rfatt	rfatt

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_calibset(struct bwn_mac *mac,

```
....
2539.       memcpy(&cal->rfatt, rfatt, sizeof(*rfatt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=250
Status	New

The size of the buffer used by bwn_lo_calibset in loctl, at line 2502 of freebsd-src-3/if_bwn_phy_g.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwn_lo_calibset passes to loctl, at line 2502 of freebsd-src-3/if_bwn_phy_g.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2540	2540
Object	loctl	loctl

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_calibset(struct bwn_mac *mac,

```
....
2540.       memcpy(&cal->ctl, &loctl, sizeof(loctl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=251
Status	New

The size of the buffer used by irdma_get_addr_info in ->, at line 111 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_get_addr_info passes to ->, at line 111 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	117	117
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_get_addr_info(struct irdma_cm_node *cm_node,

```
....
117.        memcpy(cm_info->loc_addr, cm_node->loc_addr, sizeof(cm_info->loc_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=252
Status New

The size of the buffer used by irdma_get_addr_info in ->, at line 111 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_get_addr_info passes to ->, at line 111 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	118	118
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_get_addr_info(struct irdma_cm_node *cm_node,

```
....
118.        memcpy(cm_info->rem_addr, cm_node->rem_addr, sizeof(cm_info->rem_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=253
Status New

The size of the buffer used by irdma_get_cmevent_info in ->, at line 176 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that irdma_get_cmevent_info passes to ->, at line 176 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	181	181
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_get_cmevent_info(struct irdma_cm_node *cm_node,

```
....
181.                sizeof(event->local_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=254
Status New

The size of the buffer used by irdma_get_cmevent_info in ->, at line 176 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_get_cmevent_info passes to ->, at line 176 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	183	183
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_get_cmevent_info(struct irdma_cm_node *cm_node,

```
....
183.                sizeof(event->remote_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=255
Status New

The size of the buffer used by irdma_create_event in Namespace1421959737, at line 270 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that irdma_create_event passes to Namespace1421959737, at line 270 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	286	286
Object	Namespace1421959737	Namespace1421959737

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_create_event(struct irdma_cm_node *cm_node,

```
....
286.                sizeof(event->cm_info.rem_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=256
Status	New

The size of the buffer used by irdma_create_event in Namespace1421959737, at line 270 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_create_event passes to Namespace1421959737, at line 270 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	288	288
Object	Namespace1421959737	Namespace1421959737

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_create_event(struct irdma_cm_node *cm_node,

```
....
288.                sizeof(event->cm_info.loc_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=257
Status	New

The size of the buffer used by irdma_del_multiple_qhash in ->, at line 1570 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that irdma_del_multiple_qhash passes to ->, at line 1570 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	1598	1598
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_del_multiple_qhash(struct irdma_device *iwdev,

```
....
1598.                    sizeof(cm_info->loc_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=258
Status	New

The size of the buffer used by irdma_add_mqh_ifa_cb in ->, at line 1698 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_add_mqh_ifa_cb passes to ->, at line 1698 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	1745	1745
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_add_mqh_ifa_cb(void *arg, struct ifaddr *ifa, u_int count)

```
....
1745.                sizeof(cm_info->loc_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=259
Status	New

The size of the buffer used by irdma_dec_refcnt_listen in Namespace1421959737, at line 1852 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that irdma_dec_refcnt_listen passes to Namespace1421959737, at line 1852 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	1903	1903
Object	Namespace1421959737	Namespace1421959737

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_dec_refcnt_listen(struct irdma_cm_core *cm_core,

```
....
1903.              memcpy(nfo.loc_addr, listener->loc_addr,
sizeof(nfo.loc_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=260
Status New

The size of the buffer used by irdma_cm_create_ah in Namespace1421959737, at line 2040 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_cm_create_ah passes to Namespace1421959737, at line 2040 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	2065	2065
Object	Namespace1421959737	Namespace1421959737

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_cm_create_ah(struct irdma_cm_node *cm_node, bool wait)

```
....
2065.                    sizeof(ah_info.dest_ip_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=261
Status New

The size of the buffer used by irdma_cm_create_ah in Namespace1421959737, at line 2040 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that irdma_cm_create_ah passes to Namespace1421959737, at line 2040 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	2067	2067
Object	Namespace1421959737	Namespace1421959737

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_cm_create_ah(struct irdma_cm_node *cm_node, bool wait)

```
....
2067.                    sizeof(ah_info.src_ip_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=262
Status New

The size of the buffer used by irdma_make_cm_node in ->, at line 2111 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_make_cm_node passes to ->, at line 2111 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	2151	2151
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_make_cm_node(struct irdma_cm_core *cm_core, struct irdma_device *iwdev,

```
....
2151.       memcpy(cm_node->loc_addr, cm_info->loc_addr, sizeof(cm_node->loc_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=263
Status New

The size of the buffer used by irdma_make_cm_node in ->, at line 2111 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_make_cm_node passes to ->, at line 2111 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	2152	2152
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_make_cm_node(struct irdma_cm_core *cm_core, struct irdma_device *iwdev,

```
....
2152.       memcpy(cm_node->rem_addr, cm_info->rem_addr, sizeof(cm_node->rem_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=264
Status New

The size of the buffer used by irdma_make_listen_node in ->, at line 2788 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_make_listen_node passes to ->, at line 2788 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	2814	2814
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_make_listen_node(struct irdma_cm_core *cm_core,

```
....
2814.                       sizeof(listener->loc_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=265
Status New

The size of the buffer used by irdma_init_tcp_ctx in ->, at line 3168 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_init_tcp_ctx passes to ->, at line 3168 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	3219	3219
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_init_tcp_ctx(struct irdma_cm_node *cm_node,

```
....
3219.                    sizeof(tcp_info->dest_ip_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=266
Status	New

The size of the buffer used by irdma_init_tcp_ctx in ->, at line 3168 of freebsd-src-3/irdma_cm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that irdma_init_tcp_ctx passes to ->, at line 3168 of freebsd-src-3/irdma_cm.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	3221	3221
Object	->	->

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_init_tcp_ctx(struct irdma_cm_node *cm_node,

```
....
3221.                    sizeof(tcp_info->local_ipaddr));
```

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=1060099&projectid=60089&pathid=1406
Status	New

The variable declared in ptr at freebsd-src-3/addrtoname.c in line 1282 is not initialized when it is used by ptr at freebsd-src-3/addrtoname.c in line 1282.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	1285	1296
Object	ptr	ptr

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method newhnamemem(netdissect_options *ndo)

```
....
1285.       static struct hnamemem *ptr = NULL;
....
1296.       p = ptr++;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1407
Status	New

The variable declared in ptr at freebsd-src-3/addrtoname.c in line 1282 is not initialized when it is used by ptr at freebsd-src-3/addrtoname.c in line 1282.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	1285	1290
Object	ptr	ptr

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method newhnamemem(netdissect_options *ndo)

```
....
1285.       static struct hnamemem *ptr = NULL;
....
1290.             ptr = (struct hnamemem *)calloc(num, sizeof (*ptr));
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1408
Status	New

The variable declared in ptr at freebsd-src-3/addrtoname.c in line 1302 is not initialized when it is used by ptr at freebsd-src-3/addrtoname.c in line 1302.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	1305	1316
Object	ptr	ptr

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method newh6namemem(netdissect_options *ndo)

```
....
1305.       static struct h6namemem *ptr = NULL;
....
1316.       p = ptr++;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1409
Status	New

The variable declared in ptr at freebsd-src-3/addrtoname.c in line 1302 is not initialized when it is used by ptr at freebsd-src-3/addrtoname.c in line 1302.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	1305	1310
Object	ptr	ptr

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method newh6namemem(netdissect_options *ndo)

```
....
1305.       static struct h6namemem *ptr = NULL;
....
1310.             ptr = (struct h6namemem *)calloc(num, sizeof (*ptr));
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1410
Status	New

The variable declared in erp at freebsd-src-3/eap.c in line 684 is not initialized when it is used by erp at freebsd-src-3/eap.c in line 684.

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	697	718
Object	erp	erp

Code Snippet
File Name freebsd-src-3/eap.c
Method void eap_peer_erp_init(struct eap_sm *sm, u8 *ext_session_id,

```
....
697.        struct eap_erp_key *erp = NULL;
....
718.        erp = os_zalloc(sizeof(*erp) + nai_buf_len);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1411
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	101	2211
Object	p_StatsObj	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

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

File Name	freebsd-src-3/fm_cc.c
Method	static void FillAdOfTypeResult(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1412
Status	New

The variable declared in p_AdTableNew at freebsd-src-3/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	2519	2211
Object	p_AdTableNew	p_AdNewPtr

Code Snippet

File Name	freebsd-src-3/fm_cc.c
Method	static t_Error BuildNewNodeCommonPart(

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

File Name	freebsd-src-3/fm_cc.c
Method	static void FillAdOfTypeResult(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1413
Status	New

The variable declared in h_Ad at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination

File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1264	2211
Object	h_Ad	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/fm_cc.c
Method static void FillAdOfTypeResult(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1414
Status	New

The variable declared in h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1250	2211
Object	h_KeysMatchTable	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/fm_cc.c
Method static void FillAdOfTypeResult(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1415
Status	New

The variable declared in p_GlblMask at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1243	2211
Object	p_GlblMask	p_AdNewPtr

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/fm_cc.c

Method static void FillAdOfTypeResult(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1416
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	101	308
Object	p_StatsObj	p_AdNewPtr

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

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

File Name freebsd-src-3/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1417
Status New

The variable declared in p_AdTableNew at freebsd-src-3/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	2519	308
Object	p_AdTableNew	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeCommonPart(

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

File Name freebsd-src-3/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1418
Status New

The variable declared in h_Ad at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1264	308
Object	h_Ad	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/fm_cc.c
Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1419
Status	New

The variable declared in h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1250	308
Object	h_KeysMatchTable	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1420
Status	New

The variable declared in p_GlblMask at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1243	308
Object	p_GlblMask	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/fm_cc.c

Method static void FillAdOfTypeContLookup(t_Handle h_Ad,

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

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1421
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	4819	107
Object	p_StatsObj	p_StatsObj

Code Snippet
File Name freebsd-src-3/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 freebsd-src-3/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 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1422
Status	New

The variable declared in p_GlblMask at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1243	107
Object	p_GlblMask	p_StatsObj

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1423
Status	New

The variable declared in h_Ad at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1264	107
Object	h_Ad	p_StatsObj

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1424
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4776	107
Object	p_StatsObj	p_StatsObj

Code Snippet

File Name freebsd-src-3/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 freebsd-src-3/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 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1425
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 99 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	101	107
Object	p_StatsObj	p_StatsObj

Code Snippet
File Name freebsd-src-3/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 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1426
Status	New

The variable declared in h_StatsFLRs at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1272	107
Object	h_StatsFLRs	p_StatsObj

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1427
Status	New

The variable declared in h_AdTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1257	107
Object	h_AdTable	p_StatsObj

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1428
Status	New

The variable declared in h_Spinlock at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1278	107
Object	h_Spinlock	p_StatsObj

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1429
Status	New

The variable declared in h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_StatsObj at freebsd-src-3/fm_cc.c in line 99.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	1250	107
Object	h_KeysMatchTable	p_StatsObj

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1430
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by p_CcNodeInfo at freebsd-src-3/fm_cc.c in line 1202.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4819	1209
Object	p_StatsObj	p_CcNodeInfo

Code Snippet
File Name freebsd-src-3/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 freebsd-src-3/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 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1431
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 99 is not initialized when it is used by p_CcNodeInfo at freebsd-src-3/fm_cc.c in line 1202.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	101	1209
Object	p_StatsObj	p_CcNodeInfo

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

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

File Name freebsd-src-3/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 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1432
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by p_CcNodeInfo at freebsd-src-3/fm_cc.c in line 1202.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4776	1209
Object	p_StatsObj	p_CcNodeInfo

Code Snippet

File Name freebsd-src-3/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 freebsd-src-3/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 28:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1433
Status New

The variable declared in p_GlblMask at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_CcNodeInfo at freebsd-src-3/fm_cc.c in line 1202.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1243	1209
Object	p_GlblMask	p_CcNodeInfo

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 29:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1434

Status	New

The variable declared in h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_CcNodeInfo at freebsd-src-3/fm_cc.c in line 1202.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1250	1209
Object	h_KeysMatchTable	p_CcNodeInfo

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1435
Status	New

The variable declared in p_CcNodeInfo at freebsd-src-3/fm_cc.c in line 1202 is not initialized when it is used by p_CcNodeInfo at freebsd-src-3/fm_cc.c in line 1216.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1205	1222
Object	p_CcNodeInfo	p_CcNodeInfo

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_CcNodeInformation * DequeueAdditionalInfoFromRelevantLst(

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

File Name	freebsd-src-3/fm_cc.c
Method	void ReleaseLst(t_List *p_List)

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

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1436
Status	New

The variable declared in h_TmpAd at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1265	4707
Object	h_TmpAd	h_KeysMatchTable

Code Snippet

File Name	freebsd-src-3/fm_cc.c
Method	static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name	freebsd-src-3/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=1060099&projectid=60089&pathid=1437
Status	New

The variable declared in h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1250	4707
Object	h_KeysMatchTable	h_KeysMatchTable

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1438
Status	New

The variable declared in h_AdTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1257	4707
Object	h_AdTable	h_KeysMatchTable

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1439
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 99 is not initialized when it is used by h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	101	4707
Object	p_StatsObj	h_KeysMatchTable

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1440
Status	New

The variable declared in p_AdTableNew at freebsd-src-3/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	2519	2198
Object	p_AdTableNew	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeCommonPart(

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1441
Status	New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	101	2198
Object	p_StatsObj	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1442
Status	New

The variable declared in p_GlblMask at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1243	2198
Object	p_GlblMask	p_AdNewPtr

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1443
Status	New

The variable declared in h_Ad at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1264	2198
Object	h_Ad	p_AdNewPtr

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1444
Status	New

The variable declared in h_Spinlock at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 2169.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1278	2198
Object	h_Spinlock	p_AdNewPtr

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1445
Status	New

The variable declared in p_AdTableNew at freebsd-src-3/fm_cc.c in line 2487 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	2519	295
Object	p_AdTableNew	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeCommonPart(

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1446
Status New

The variable declared in p_StatsObj at freebsd-src-3/fm_cc.c in line 99 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	101	295
Object	p_StatsObj	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static __inline__ t_FmPcdStatsObj* DequeueStatsObj(t_List *p_List)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1447
Status	New

The variable declared in p_GlblMask at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1243	295
Object	p_GlblMask	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1448
Status	New

The variable declared in h_Ad at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c

Line	1264	295
Object	h_Ad	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1449
Status	New

The variable declared in h_Spinlock at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by p_AdNewPtr at freebsd-src-3/fm_cc.c in line 266.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1278	295
Object	h_Spinlock	p_AdNewPtr

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1450
Status	New

The variable declared in h_AdTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1257	4719
Object	h_AdTable	h_AdTable

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1451
Status	New

The variable declared in h_StatsFLRs at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1272	4719
Object	h_StatsFLRs	h_AdTable

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1452
Status	New

The variable declared in h_Ad at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1264	4719
Object	h_Ad	h_AdTable

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1453
Status	New

The variable declared in p_GlblMask at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1243	4719
Object	p_GlblMask	h_AdTable

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1454
Status	New

The variable declared in h_KeysMatchTable at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1250	4719
Object	h_KeysMatchTable	h_AdTable

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1455
Status	New

The variable declared in h_TmpAd at freebsd-src-3/fm_cc.c in line 1233 is not initialized when it is used by h_AdTable at freebsd-src-3/fm_cc.c in line 4324.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	1265	4719
Object	h_TmpAd	h_AdTable

Code Snippet	
File Name	freebsd-src-3/fm_cc.c
Method	static void DeleteNode(t_FmPcdCcNode *p_CcNode)

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

File Name	freebsd-src-3/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);
```

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=1060099&projectid=60089&pathid=921
Status	New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	375	375
Object	outfile	outfile

Code Snippet
File Name freebsd-src-3/hxtool.c
Method cms_create_sd(struct cms_create_sd_options *opt, int argc, char **argv)

```
....
375.        asprintf(&outfile, "%s.%s", infile,
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=922
Status New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	2130	2130
Object	dir	dir

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method int main(int argc, char *argv[])

```
....
2130.                   DIR *dir = opendir(ctrl_iface_dir);
```

Memory Leak\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=923
Status New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	310	310
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method ipaddr_string(netdissect_options *ndo, const u_char *ap)

```
....
310.                    p->name = strdup(hp->h_name);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=924
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	323	323
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method ipaddr_string(netdissect_options *ndo, const u_char *ap)

```
....
323.        p->name = strdup(intoa(addr));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=925
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	373	373
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
373.                    p->name = strdup(hp->h_name);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=926
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	387	387
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
387.         p->name = strdup(cp);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=927
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	454	454
Object	e_nxt	e_nxt

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_emem(netdissect_options *ndo, const u_char *ep)

```
....
454.         tp->e_nxt = (struct enamemem *)calloc(1, sizeof(*tp));
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=928
Status	New

	Source	Destination

File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	499	499
Object	bs_bytes	bs_bytes

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_bytestring(netdissect_options *ndo, const u_char *bs,

```
....
499.        tp->bs_bytes = (u_char *) calloc(1, nlen);
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=929
Status New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	506	506
Object	bs_nxt	bs_nxt

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_bytestring(netdissect_options *ndo, const u_char *bs,

```
....
506.        tp->bs_nxt = (struct bsnamemem *)calloc(1, sizeof(*tp));
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=930
Status New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	547	547
Object	e_nsap	e_nsap

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_nsap(netdissect_options *ndo, const u_char *nsap,

```
....
547.        tp->e_nsap = (u_char *)malloc(nsap_length + 1);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=931
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	552	552
Object	e_nxt	e_nxt

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_nsap(netdissect_options *ndo, const u_char *nsap,

```
....
552.        tp->e_nxt = (struct enamemem *)calloc(1, sizeof(*tp));
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=932
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	580	580
Object	p_nxt	p_nxt

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method lookup_protoid(netdissect_options *ndo, const u_char *pi)

```
....
580.        tp->p_nxt = (struct protoidmem *)calloc(1, sizeof(*tp));
```

Memory Leak\Path 13:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=933
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	611	611
Object	e_name	e_name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method etheraddr_string(netdissect_options *ndo, const uint8_t *ep)

```
....
611.                    tp->e_name = strdup(buf2);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=934
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	632	632
Object	e_name	e_name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method etheraddr_string(netdissect_options *ndo, const uint8_t *ep)

```
....
632.        tp->e_name = strdup(buf);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=935
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	661	661

Object	bs_name	bs_name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method le64addr_string(netdissect_options *ndo, const uint8_t *ep)

```
....
661.        tp->bs_name = strdup(buf);
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=936
Status New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	690	690
Object	cp	cp

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method linkaddr_string(netdissect_options *ndo, const uint8_t *ep,

```
....
690.        tp->bs_name = cp = (char *)malloc(len*3);
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=937
Status New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	719	719
Object	cp	cp

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method isonsap_string(netdissect_options *ndo, const uint8_t *nsap,

```
....
719.        tp->e_name = cp = (char
*)malloc(sizeof("xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx"));
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=938
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	750	750
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method tcpport_string(netdissect_options *ndo, u_short port)

```
....
750.        tp->name = strdup(buf);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=939
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	772	772
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method udpport_string(netdissect_options *ndo, u_short port)

```
....
772.        tp->name = strdup(buf);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=940
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	801	801
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method ipxsap_string(netdissect_options *ndo, u_short port)

```
....
801.         tp->name = strdup(buf);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=941
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	830	830
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method init_servarray(netdissect_options *ndo)

```
....
830.                     table->name = strdup(buf);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=942
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c

Line	832	832
Object	name	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method init_servarray(netdissect_options *ndo)

```
....
832.                    table->name = strdup(sv->s_name);
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=943
Status New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	911	911
Object	p_name	p_name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method init_protoidarray(netdissect_options *ndo)

```
....
911.                tp->p_name = strdup(eproto_db[i].s);
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=944
Status New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	989	989
Object	e_name	e_name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method init_etherarray(netdissect_options *ndo)

```
....
989.                    tp->e_name = strdup(name);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=945
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	1290	1290
Object	ptr	ptr

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method newhnamemem(netdissect_options *ndo)

```
....
1290.             ptr = (struct hnamemem *)calloc(num, sizeof (*ptr));
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=946
Status	New

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	1310	1310
Object	ptr	ptr

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method newh6namemem(netdissect_options *ndo)

```
....
1310.             ptr = (struct h6namemem *)calloc(num, sizeof (*ptr));
```

Memory Leak\Path 27:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=947
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	143	143
Object	appends	appends

Code Snippet
File Name freebsd-src-3/compile.c
Method compile(void)

```
....
143.        else if ((appends = malloc(sizeof(struct s_appends) *
appendnum)) ==
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=948
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	146	146
Object	match	match

Code Snippet
File Name freebsd-src-3/compile.c
Method compile(void)

```
....
146.        if ((match = malloc((maxnsub + 1) * sizeof(regmatch_t))) ==
NULL)
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=949
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c

Line	184	184
Object	cmd	cmd

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_stream(struct s_command **link)

```
....
184.                if ((*link = cmd = malloc(sizeof(struct s_command)))
== NULL)
```

Memory Leak\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=950
Status New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	195	195
Object	a1	a1

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_stream(struct s_command **link)

```
....
195.                    if ((cmd->a1 = malloc(sizeof(struct s_addr))) ==
NULL)
```

Memory Leak\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=951
Status New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	203	203
Object	a2	a2

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_stream(struct s_command **link)

```
....
203.                            if ((cmd->a2 = malloc(sizeof(struct
s_addr)))
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=952
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	324	324
Object	s	s

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_stream(struct s_command **link)

```
....
324.                    if ((cmd->u.s = calloc(1, sizeof(struct
s_subst))) == NULL)
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=953
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	548	548
Object	rep	rep

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_re(char *re, int case_insensitive)

```
....
548.        if ((rep = malloc(sizeof(regex_t))) == NULL)
```

Memory Leak\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=954
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	579	579
Object	text	text

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_subst(char *p, struct s_subst *s)

```
....
579.        if ((text = malloc(asize)) == NULL)
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=955
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	749	749
Object	wfile	wfile

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_flags(char *p, struct s_subst *s)

```
....
749.                    s->wfile = strdup(wfile);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=956
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c

Line	778	778
Object	y	y

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_tr(char *p, struct s_tr **py)

```
....
778.        if ((*py = y = malloc(sizeof(*y))) == NULL)
```

Memory Leak\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=957
Status New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	867	867
Object	text	text

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_text(void)

```
....
867.        if ((text = malloc(asize)) == NULL)
```

Memory Leak\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=958
Status New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	970	970
Object	p	p

Code Snippet
File Name freebsd-src-3/compile.c
Method duptoeol(char *s, const char *ctype)

```
....
970.        if ((p = malloc(len)) == NULL)
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=959
Status	New

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	1026	1026
Object	lh	lh

Code Snippet
File Name freebsd-src-3/compile.c
Method enterlabel(struct s_command *cp)

```
....
1026.       if ((lh = malloc(sizeof *lh)) == NULL)
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=960
Status	New

	Source	Destination
File	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c
Line	279	279
Object	doc	doc

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetchMakeURL(const char *scheme, const char *host, int port, const char *doc,

```
....
279.        if ((u->doc = strdup(doc ? doc : "/")) == NULL) {
```

Memory Leak\Path 41:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=961
Status	New

	Source	Destination
File	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c
Line	448	448
Object	doc	doc

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetchParseURL(const char *URL)

```
....
448.              if ((doc = malloc(strlen(p) * 3 + 1)) == NULL) {
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=962
Status	New

	Source	Destination
File	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c
Line	464	464
Object	doc	doc

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetchParseURL(const char *URL)

```
....
464.          } else if ((u->doc = strdup(p)) == NULL) {
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=963
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	956	956

Object	dir	dir

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static void hostapd_cli_get_interfaces(struct wpa_ctrl *ctrl,

```
....
956.        dir = opendir(ctrl_iface_dir);
```

Memory Leak\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=964
Status New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	975	975
Object	dir	dir

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static void hostapd_cli_list_interfaces(struct wpa_ctrl *ctrl)

```
....
975.        dir = opendir(ctrl_iface_dir);
```

Memory Leak\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=965
Status New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	161	161
Object	data	data

Code Snippet
File Name freebsd-src-3/hxtool.c
Method pem_reader(hx509_context contextp, const char *type,

```
....
161.      p->os->data = malloc(length);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=966
Status	New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1260	1260
Object	p	p

Code Snippet
File Name freebsd-src-3/hxtool.c
Method get_key(const char *fn, const char *type, int optbits,

```
....
1260.       p0 = p = malloc(len);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=967
Status	New

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2533	2533
Object	cal	cal

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_lo_calibset(struct bwn_mac *mac,

```
....
2533.       cal = malloc(sizeof(*cal), M_DEVBUF, M_NOWAIT | M_ZERO);
```

Memory Leak\Path 48:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=968
Status	New

	Source	Destination
File	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c
Line	642	642
Object	mvp	mvp

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_vap_create(struct ieee80211com *ic, const char name[IFNAMSIZ], int unit,

```
....
642.        mvp = malloc(sizeof(struct mwl_vap), M_80211_VAP, M_WAITOK |
M_ZERO);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=969
Status	New

	Source	Destination
File	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c
Line	2039	2039
Object	bf	bf

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_txdma_setup(struct mwl_softc *sc, struct mwl_txq *txq)

```
....
2039.       bf = malloc(bsize, M_MWLDEV, M_NOWAIT | M_ZERO);
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=970
Status	New

	Source	Destination
File	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c

Line	2159	2159
Object	bf	bf

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_rxdma_setup(struct mwl_softc *sc)

```
....
2159.       bf = malloc(bsize, M_MWLDEV, M_NOWAIT | M_ZERO);
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=522
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-3/compat.c may result with a crash.

	Source	Destination
File	freebsd-src-3/compat.c	freebsd-src-3/compat.c
Line	158	158
Object	cp	cp

Code Snippet
File Name freebsd-src-3/compat.c
Method compat_kex_proposal(struct ssh *ssh, const char *p)

```
....
158.                free(cp);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=523
Status	New

Calling free() (line 1062) on a variable that was not dynamically allocated (line 1062) in file freebsd-src-3/compile.c may result with a crash.

	Source	Destination

File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	1073	1073
Object	lh	lh

Code Snippet
File Name freebsd-src-3/compile.c
Method uselabel(void)

```
....
1073.                   free(lh);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=524
Status	New

Calling free() (line 317) on a variable that was not dynamically allocated (line 317) in file freebsd-src-3/freebsd32_misc.c may result with a crash.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	338	338
Object	buf	buf

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd4_freebsd32_getfsstat(struct thread *td,

```
....
338.                free(buf, M_STATFS);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=525
Status	New

Calling free() (line 1648) on a variable that was not dynamically allocated (line 1648) in file freebsd-src-3/freebsd32_misc.c may result with a crash.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	1694	1694

Object	to	to

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_sendmsg(struct thread *td, struct freebsd32_sendmsg_args *uap)

```
....
1694.              free(to, M_SONAME);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=526
Status New

Calling free() (line 179) on a variable that was not dynamically allocated (line 179) in file freebsd-src-3/hxtool.c may result with a crash.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	301	301
Object	str	str

Code Snippet
File Name freebsd-src-3/hxtool.c
Method cms_verify_sd(struct cms_verify_sd_options *opt, int argc, char **argv)

```
....
301.         free(str);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=527
Status New

Calling free() (line 334) on a variable that was not dynamically allocated (line 334) in file freebsd-src-3/hxtool.c may result with a crash.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	352	352
Object	signer_name	signer_name

Code Snippet	
File Name	freebsd-src-3/hxtool.c
Method	print_signer(hx509_context contextp, void *ctx, hx509_cert cert)

```
....
352.        free(signer_name);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=528
Status	New

Calling free() (line 1449) on a variable that was not dynamically allocated (line 1449) in file freebsd-src-3/hxtool.c may result with a crash.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1476	1476
Object	s	s

Code Snippet	
File Name	freebsd-src-3/hxtool.c
Method	crypto_available(struct crypto_available_options *opt, int argc, char **argv)

```
....
1476.        free(s);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=529
Status	New

Calling free() (line 1485) on a variable that was not dynamically allocated (line 1485) in file freebsd-src-3/hxtool.c may result with a crash.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1512	1512
Object	s	s

Code Snippet	
File Name	freebsd-src-3/hxtool.c
Method	crypto_select(struct crypto_select_options *opt, int argc, char **argv)

```
....
1512.       free(s);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=530
Status	New

Calling free() (line 1521) on a variable that was not dynamically allocated (line 1521) in file freebsd-src-3/hxtool.c may result with a crash.

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1548	1548
Object	p	p

Code Snippet
File Name freebsd-src-3/hxtool.c
Method hxtool_hex(struct hex_options *opt, int argc, char **argv)

```
....
1548.           free(p);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=531
Status	New

Calling free() (line 467) on a variable that was not dynamically allocated (line 467) in file freebsd-src-3/if_bwn_phy_g.c may result with a crash.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	476	476
Object	cal	cal

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_phy_g_exit(struct bwn_mac *mac)

```
....
476.                free(cal, M_DEVBUF);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=532
Status	New

Calling free() (line 757) on a variable that was not dynamically allocated (line 757) in file freebsd-src-3/if_bwn_phy_g.c may result with a crash.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	797	797
Object	cal	cal

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_phy_g_task_15s(struct bwn_mac *mac)

```
....
797.                free(cal, M_DEVBUF);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=533
Status	New

Calling free() (line 2571) on a variable that was not dynamically allocated (line 2571) in file freebsd-src-3/if_bwn_phy_g.c may result with a crash.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2614	2614
Object	cal	cal

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_phy_g_dc_lookup_init(struct bwn_mac *mac, uint8_t update)

```
....
2614.             free(cal, M_DEVBUF);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=534
Status	New

Calling free() (line 719) on a variable that was not dynamically allocated (line 719) in file freebsd-src-3/if_mwl.c may result with a crash.

	Source	Destination
File	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c
Line	754	754
Object	mvp	mvp

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_vap_delete(struct ieee80211vap *vap)

```
....
754.         free(mvp, M_80211_VAP);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=535
Status	New

Calling free() (line 110) on a variable that was not dynamically allocated (line 110) in file freebsd-src-3/iter_utils.c may result with a crash.

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	124	124
Object	nm	nm

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method caps_white_apply_cfg(rbtree_type* ntree, struct config_file* cfg)

```
....
124.                    free(nm);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=536
Status	New

Calling free() (line 173) on a variable that was not dynamically allocated (line 173) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	212	212
Object	ns	ns

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_tcp_start(ldns_resolver *res, ldns_pkt *qpkt, int nameserver) {

```
....
212.      free(ns);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=537
Status	New

Calling free() (line 173) on a variable that was not dynamically allocated (line 173) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	217	217
Object	ns	ns

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_tcp_start(ldns_resolver *res, ldns_pkt *qpkt, int nameserver) {

```
....
217.        free(ns);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=538
Status	New

Calling free() (line 226) on a variable that was not dynamically allocated (line 226) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	242	242
Object	data	data

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_tcp_read(ldns_pkt **answer, ldns_resolver *res) {

```
....
242.        free(data);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=539
Status	New

Calling free() (line 392) on a variable that was not dynamically allocated (line 392) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	398	398
Object	str	str

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method print_rr_type(ldns_rr_type type) {

```
....
398.        free(str);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=540
Status	New

Calling free() (line 403) on a variable that was not dynamically allocated (line 403) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	409	409
Object	str	str

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method print_rr_class(ldns_rr_class cls) {

```
....
409.        free(str);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=541
Status	New

Calling free() (line 414) on a variable that was not dynamically allocated (line 414) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	420	420
Object	str	str

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method print_rdf(ldns_rdf *rdf) {

```
....
420.        free(str);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=542
Status	New

Calling free() (line 425) on a variable that was not dynamically allocated (line 425) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	432	432
Object	str	str

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method print_rdf_nodot(ldns_rdf *rdf) {

```
....
432.        free(str);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=543
Status	New

Calling free() (line 558) on a variable that was not dynamically allocated (line 558) in file freebsd-src-3/ldns-host.c may result with a crash.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	564	564
Object	from	from

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method print_received_line(ldns_resolver *res, ldns_pkt *pkt) {

```
....
564.        free(from);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=544
Status	New

Calling free() (line 626) on a variable that was not dynamically allocated (line 626) in file freebsd-src-3/mmc_da.c may result with a crash.

	Source	Destination
File	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c
Line	640	640
Object	part	part

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method sddacleanup(struct cam_periph *periph)

```
....
640.                    free(part, M_DEVBUF);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=545
Status	New

Calling free() (line 626) on a variable that was not dynamically allocated (line 626) in file freebsd-src-3/mmc_da.c may result with a crash.

	Source	Destination
File	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c
Line	644	644
Object	softc	softc

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method sddacleanup(struct cam_periph *periph)

```
....
644.        free(softc, M_DEVBUF);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=546
Status	New

Calling free() (line 1955) on a variable that was not dynamically allocated (line 1955) in file freebsd-src-3/pkinit.c may result with a crash.

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	2022	2022
Object	str	str

Code Snippet
File Name freebsd-src-3/pkinit.c
Method krb5_kdc_pk_initialize(krb5_context context,

```
....
2022.                    free(str);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=547
Status	New

Calling free() (line 1955) on a variable that was not dynamically allocated (line 1955) in file freebsd-src-3/pkinit.c may result with a crash.

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	2051	2051
Object	fn	fn

Code Snippet
File Name freebsd-src-3/pkinit.c
Method krb5_kdc_pk_initialize(krb5_context context,

```
....
2051.       free(fn);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=548
Status	New

Calling free() (line 112) on a variable that was not dynamically allocated (line 112) in file freebsd-src-3/pkinit.c may result with a crash.

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	146	146
Object	buf	buf

Code Snippet
File Name freebsd-src-3/pkinit.c
Method pk_check_pkauthenticator(krb5_context context,

```
....
146.       free(buf);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=549
Status	New

Calling free() (line 1241) on a variable that was not dynamically allocated (line 1241) in file freebsd-src-3/pkinit.c may result with a crash.

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1477	1477
Object	buf	buf

Code Snippet
File Name freebsd-src-3/pkinit.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1477.           free(buf);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=550
Status	New

Calling free() (line 1241) on a variable that was not dynamically allocated (line 1241) in file freebsd-src-3/pkinit.c may result with a crash.

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1489	1489
Object	buf	buf

Code Snippet
File Name freebsd-src-3/pkinit.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1489.       free(buf);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=551
Status	New

Calling free() (line 143) on a variable that was not dynamically allocated (line 143) in file freebsd-src-3/print.c may result with a crash.

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	148	148
Object	str	str

Code Snippet
File Name freebsd-src-3/print.c
Method hx509_oid_print(const heim_oid *oid, hx509_vprint_func func, void *ctx)

```
....
148.        free(str);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=552
Status	New

Calling free() (line 277) on a variable that was not dynamically allocated (line 277) in file freebsd-src-3/print.c may result with a crash.

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	315	315
Object	id	id

Code Snippet
File Name freebsd-src-3/print.c
Method check_subjectKeyIdentifier(hx509_validate_ctx ctx,

```
....
315.            free(id);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=553
Status	New

Calling free() (line 325) on a variable that was not dynamically allocated (line 325) in file freebsd-src-3/print.c may result with a crash.

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	357	357
Object	id	id

Code Snippet
File Name freebsd-src-3/print.c
Method check_authorityKeyIdentifier(hx509_validate_ctx ctx,

```
....
357.            free(id);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=554
Status	New

Calling free() (line 365) on a variable that was not dynamically allocated (line 365) in file freebsd-src-3/print.c may result with a crash.

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	407	407
Object	str	str

Code Snippet
File Name freebsd-src-3/print.c
Method check_extKeyUsage(hx509_validate_ctx ctx,

```
....
407.        free(str);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=555
Status	New

Calling free() (line 477) on a variable that was not dynamically allocated (line 477) in file freebsd-src-3/print.c may result with a crash.

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	524	524
Object	s	s

Code Snippet
File Name freebsd-src-3/print.c
Method check_CRLDistributionPoints(hx509_validate_ctx ctx,

```
....
524.                    free(s);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=556
Status	New

Calling free() (line 561) on a variable that was not dynamically allocated (line 561) in file freebsd-src-3/print.c may result with a crash.

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	628	628
Object	s	s

Code Snippet
File Name freebsd-src-3/print.c
Method check_altName(hx509_validate_ctx ctx,

```
....
628.            free(s);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=557
Status	New

Calling free() (line 715) on a variable that was not dynamically allocated (line 715) in file freebsd-src-3/print.c may result with a crash.

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	743	743
Object	str	str

Code Snippet
File Name freebsd-src-3/print.c
Method check_authorityInfoAccess(hx509_validate_ctx ctx,

```
....
743.        free(str);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=558
Status	New

Calling free() (line 383) on a variable that was not dynamically allocated (line 383) in file freebsd-src-3/t_regex_att.c may result with a crash.

	Source	Destination
File	freebsd-src-3/t_regex_att.c	freebsd-src-3/t_regex_att.c
Line	399	399
Object	line	line

Code Snippet
File Name freebsd-src-3/t_regex_att.c
Method att_test(const struct atf_tc *tc, const char *data_name)

```
....
399.            != NULL; free(line)) {
```

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=1060099&projectid=60089&pathid=491
Status	New

The application performs an illegal operation in main_thread, in freebsd-src-3/pkt-gen.c. In line 2710, the program attempts to divide by nsamples, 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 nsamples in main_thread of freebsd-src-3/pkt-gen.c, at line 2710.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	2766	2766
Object	nsamples	nsamples

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method main_thread(struct glob_arg *g)

```
....
2766.                    ppsavg /= nsamples;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=492
Status	New

The application performs an illegal operation in main_thread, in freebsd-src-3/pkt-gen.c. In line 2710, the program attempts to divide by nsamples, 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 nsamples in main_thread of freebsd-src-3/pkt-gen.c, at line 2710.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	2774	2774
Object	nsamples	nsamples

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method main_thread(struct glob_arg *g)

```
....
2774.                    ppsdev /= nsamples;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=493
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1554	1554
Object	g_fxp	g_fxp

Code Snippet	
File Name	freebsd-src-3/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=1060099&projectid=60089&pathid=494
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1565	1565
Object	g_fxp	g_fxp

Code Snippet	
File Name	freebsd-src-3/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=1060099&projectid=60089&pathid=495
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c

Line	1638	1638
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=496
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1639	1639
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=497
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination

File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1640	1640
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=498
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1665	1665
Object	scale_b	scale_b

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=499
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1666	1666
Object	scale_b	scale_b

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=500
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1691	1691
Object	g_fxp	g_fxp

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=501
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1740	1740
Object	scale_b	scale_b

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=502
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1741	1741
Object	scale_b	scale_b

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=503
Status	New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1756	1756
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=504
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1759	1759
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=505
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1762	1762
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=506
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1763	1763
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=507
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1764	1764
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=508
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1765	1765
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=509
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1770	1770
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=510
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1772	1772
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=511
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1775	1775
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=512
Status New

The application performs an illegal operation in create_pa_curve, in freebsd-src-3/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 freebsd-src-3/ar9300_paprd.c, at line 1385.

	Source	Destination
File	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1776	1776
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=513
Status New

The application performs an illegal operation in bwn_nrssi_slope_11g, in freebsd-src-3/if_bwn_phy_g.c. In line 2727, the program attempts to divide by BinaryExpr, 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 BinaryExpr in bwn_nrssi_slope_11g of freebsd-src-3/if_bwn_phy_g.c, at line 2727.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	2849	2849
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_nrssi_slope_11g(struct bwn_mac *mac)

```
....
2849.             pg->pg_nrssi_slope = 0x00400000 / (nrssi0 - nrssi1);
```

Divide By Zero\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=514
Status New

The application performs an illegal operation in main, in freebsd-src-3/pkt-gen.c. In line 2928, the program attempts to divide by tx_rate, 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 tx_rate in main of freebsd-src-3/pkt-gen.c, at line 2928.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	3363	3363
Object	tx_rate	tx_rate

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method main(int arc, char **argv)

```
....
3363.             x = ((uint64_t)1000000000 * (uint64_t)g.burst) /
(uint64_t) g.tx_rate;
```

Divide By Zero\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=515

Status	New

The application performs an illegal operation in ping_body, in freebsd-src-3/pkt-gen.c. In line 1384, the program attempts to divide by count, 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 count in ping_body of freebsd-src-3/pkt-gen.c, at line 1384.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1534	1534
Object	count	count

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method ping_body(void *data)

```
....
1534.                          (int)count, (int)t_min, (int)(av/count));
```

Divide By Zero\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=516
Status	New

The application performs an illegal operation in main_thread, in freebsd-src-3/pkt-gen.c. In line 2710, the program attempts to divide by usec, 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 usec in main_thread of freebsd-src-3/pkt-gen.c, at line 2710.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	2747	2747
Object	usec	usec

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method main_thread(struct glob_arg *g)

```
....
2747.             pps = (x.pkts*1000000 + usec/2) / usec;
```

Divide By Zero\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=600

	89&pathid=517
Status	New

The application performs an illegal operation in main_thread, in freebsd-src-3/pkt-gen.c. In line 2710, the program attempts to divide by usec, 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 usec in main_thread of freebsd-src-3/pkt-gen.c, at line 2710.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	2784	2784
Object	usec	usec

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method main_thread(struct glob_arg *g)

```
....
2784.                    norm(b3,
1000000*((double)x.bytes*8+(double)x.pkts*g->framing)/usec, normalize),
```

Divide By Zero\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=518
Status	New

The application performs an illegal operation in ssl3_enc, in freebsd-src-3/ssl3_record.c. In line 915, the program attempts to divide by bs, 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 bs in ssl3_enc of freebsd-src-3/ssl3_record.c, at line 915.

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c
Line	955	955
Object	bs	bs

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method int ssl3_enc(SSL *s, SSL3_RECORD *inrecs, size_t n_recs, int sending)

```
....
955.              i = bs - (l % bs);
```

Divide By Zero\Path 29:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=519
Status	New

The application performs an illegal operation in ssl3_enc, in freebsd-src-3/ssl3_record.c. In line 915, the program attempts to divide by bs, 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 bs in ssl3_enc of freebsd-src-3/ssl3_record.c, at line 915.

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c
Line	969	969
Object	bs	bs

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method int ssl3_enc(SSL *s, SSL3_RECORD *inrecs, size_t n_recs, int sending)

```
....
969.              if (l == 0 || l % bs != 0)
```

Divide By Zero\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=520
Status	New

The application performs an illegal operation in tls1_enc, in freebsd-src-3/ssl3_record.c. In line 1006, the program attempts to divide by bs, 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 bs in tls1_enc of freebsd-src-3/ssl3_record.c, at line 1006.

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c
Line	1145	1145
Object	bs	bs

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method int tls1_enc(SSL *s, SSL3_RECORD *recs, size_t n_recs, int sending)

```
....
1145.                  padnum = bs - (reclen[ctr] % bs);
```

Divide By Zero\Path 31:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=521
Status	New

The application performs an illegal operation in n_ssl3_mac, in freebsd-src-3/ssl3_record.c. In line 1253, the program attempts to divide by md_size, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input md_size in n_ssl3_mac of freebsd-src-3/ssl3_record.c, at line 1253.

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c
Line	1276	1276
Object	md_size	md_size

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method int n_ssl3_mac(SSL *ssl, SSL3_RECORD *rec, unsigned char *md, int sending)

```
....
1276.       npad = (48 / md_size) * md_size;
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=463
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 456 of freebsd-src-3/print-ntp.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/print-ntp.c	freebsd-src-3/print-ntp.c
Line	466	466
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/print-ntp.c

Method	p_sfix(netdissect_options *ndo,

```
....
466.        f = (int)(ff * 1000000.0);    /* Treat fraction as parts per
million */
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=464
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 32 of freebsd-src-3/dh_key.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/dh_key.c	freebsd-src-3/dh_key.c
Line	48	48
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	freebsd-src-3/dh_key.c
Method	int DH_compute_key(unsigned char *key, const BIGNUM *pub_key, DH *dh)

```
....
48.      ret -= npad;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=465
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	182	182
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method	static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
182.      frag = (unsigned int)inp_len >> (1 + n4x);
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=466
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 154 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	183	183
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
183.      last = (unsigned int)inp_len + frag - (frag << (1 + n4x));
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=467
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 402 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	465	465
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
465.              for (l = len - plen - 1; plen < len; plen++)
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=468
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 402 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	527	527
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
527.              maxpad = len - (SHA_DIGEST_LENGTH + 1);
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=469
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 402 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	585	585
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
585.                bitlen = key->md.Nl + (inp_len << 3); /* at most 18
bits */
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=470
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 402 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	532	532
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
532.                ret &= mask;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=471
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 402 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	703	703
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
703.                    cmask =
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=472
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 402 of freebsd-src-3/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	707	707
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
707.                    cmask &= ((int)(off - 1 - j)) >> (sizeof(int)
* 8 - 1);
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=473
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 150 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	179	179
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
179.      frag = (unsigned int)inp_len >> (1 + n4x);
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=474
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 150 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	180	180
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
180.      last = (unsigned int)inp_len + frag - (frag << (1 + n4x));
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=475
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 417 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	495	495
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
....
495.              for (l = len - plen - 1; plen < len; plen++)
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=476
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 417 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	539	539
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
....
539.              maxpad = len - (SHA256_DIGEST_LENGTH + 1);
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=477
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 417 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	574	574
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
....
574.                bitlen = key->md.Nl + (inp_len << 3); /* at most 18
bits */
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=478
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 417 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	544	544
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
....
544.                ret &= mask;
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=479
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 417 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	708	708
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
....
708.                    cmask =
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=480
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 417 of freebsd-src-3/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	712	712
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
....
712.                    cmask &= ((int)(off - 1 - j)) >> (sizeof(int)
* 8 - 1);
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=481
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 443 of freebsd-src-3/eap.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	506	506
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/eap.c
Method static char * eap_get_realm(struct eap_sm *sm, struct eap_peer_config *config)

```
....
506.                pos = imsi_len + 1; /* points to the beginning of the
realm */
```

Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=482
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2366 of freebsd-src-3/icmp6.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2543	2543
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2543.                len = maxlen - (p - (u_char *)ip6);
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=483
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 397 of freebsd-src-3/obj_dat.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/obj_dat.c	freebsd-src-3/obj_dat.c
Line	489	489
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/obj_dat.c
Method int OBJ_obj2txt(char *buf, int buf_len, const ASN1_OBJECT *a, int no_name)

```
....
489.                    i = (int)(l / 40);
```

Integer Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=484
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 242 of freebsd-src-3/str.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/str.c	freebsd-src-3/str.c
Line	258	258
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/str.c
Method genrange(STR *s, int was_octal)

```
....
258.                stopval = wc;
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=485
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of freebsd-src-3/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	freebsd-src-3/subr_scanf.c	freebsd-src-3/subr_scanf.c
Line	328	328
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/subr_scanf.c
Method vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
328.                                        inr -= width;
```

Integer Overflow\Path 24:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=486
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of freebsd-src-3/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	freebsd-src-3/subr_scanf.c	freebsd-src-3/subr_scanf.c
Line	336	336
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/subr_scanf.c
Method vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
336.                            inr -= width;
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=487
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of freebsd-src-3/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	freebsd-src-3/subr_scanf.c	freebsd-src-3/subr_scanf.c
Line	338	338
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/subr_scanf.c
Method vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
338.                            nread += width;
```

Integer Overflow\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=488
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 108 of freebsd-src-3/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	freebsd-src-3/subr_scanf.c	freebsd-src-3/subr_scanf.c
Line	333	333
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/subr_scanf.c
Method vsscanf(const char *inp, char const *fmt0, va_list ap)

```
....
333.                           nread += sum;
```

Integer Overflow\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=489
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2672 of freebsd-src-3/freebsd32_misc.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	2683	2683
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32___sysctlbyname(struct thread *td,

```
....
2683.             error = oldlen = 0;
```

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=1060099&projectid=60089&pathid=444
Status New

The function len in freebsd-src-3/compile.c at line 957 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	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	970	970
Object	len	len

Code Snippet
File Name freebsd-src-3/compile.c
Method duptoeol(char *s, const char *ctype)

```
....
970.        if ((p = malloc(len)) == NULL)
```

Wrong Size t Allocation\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=445
Status New

The function keylen in freebsd-src-3/crypto-pk.c at line 198 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	freebsd-src-3/crypto-pk.c	freebsd-src-3/crypto-pk.c
Line	250	250
Object	keylen	keylen

Code Snippet
File Name freebsd-src-3/crypto-pk.c
Method _krb5_pk_kdf(krb5_context context,

```
....
250.      keydata = malloc(keylen);
```

Wrong Size t Allocation\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=446
Status New

The function keylen in freebsd-src-3/crypto-pk.c at line 39 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	freebsd-src-3/crypto-pk.c	freebsd-src-3/crypto-pk.c
Line	63	63
Object	keylen	keylen

Code Snippet
File Name freebsd-src-3/crypto-pk.c
Method _krb5_pk_octetstring2key(krb5_context context,

```
....
63.      keydata = malloc(keylen);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=447
Status	New

The function len in freebsd-src-3/hxtool.c at line 1224 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	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1260	1260
Object	len	len

Code Snippet
File Name freebsd-src-3/hxtool.c
Method get_key(const char *fn, const char *type, int optbits,

```
....
1260.       p0 = p = malloc(len);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=448
Status	New

The function space in freebsd-src-3/if_mwl.c at line 2242 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	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c

Line	2249	2249
Object	space	space

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_node_alloc(struct ieee80211vap *vap, const uint8_t mac[IEEE80211_ADDR_LEN])

```
....
2249.       mn = malloc(space, M_80211_NODE, M_NOWAIT|M_ZERO);
```

Wrong Size t Allocation\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=449
Status New

The function dspathsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1199	1199
Object	dspathsiz	dspathsiz

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1199.       dspath = malloc(dspathsiz);
```

Wrong Size t Allocation\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=450
Status New

The function dshostsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1204	1204

Object	dshostsiz	dshostsiz

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1204.       dshost = malloc(dshostsiz);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=451
Status	New

The function dsaddrsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1209	1209
Object	dsaddrsiz	dsaddrsiz

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1209.       dsaddr = malloc(dsaddrsiz);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=452
Status	New

The function mdspathsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1214	1214
Object	mdspathsiz	mdspathsiz

Code Snippet	
File Name	freebsd-src-3/nfsd.c
Method	parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1214.       mdspath = malloc(mdspathsiz);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=453
Status	New

The function size in freebsd-src-3/pkinit.c at line 204 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	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	232	232
Object	size	size

Code Snippet	
File Name	freebsd-src-3/pkinit.c
Method	generate_dh_keyblock(krb5_context context,

```
....
232.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=454
Status	New

The function size in freebsd-src-3/pkinit.c at line 204 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	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	275	275
Object	size	size

Code Snippet	
File Name	freebsd-src-3/pkinit.c
Method	generate_dh_keyblock(krb5_context context,

```
....
275.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=455
Status	New

The function dspathsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1250	1250
Object	dspathsiz	dspathsiz

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1250.                    dspath = realloc(dspath, dspathsiz);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=456
Status	New

The function mdspathsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1264	1264
Object	mdspathsiz	mdspathsiz

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1264.                    mdspath = realloc(mdspath, mdspathsiz);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=457
Status	New

The function dsaddrsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1331	1331
Object	dsaddrsiz	dsaddrsiz

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1331.                    dsaddr = realloc(dsaddr, dsaddrsiz);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=458
Status	New

The function dshostsiz in freebsd-src-3/nfsd.c at line 1179 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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1343	1343
Object	dshostsiz	dshostsiz

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1343.                    dshost = realloc(dshost, dshostsiz);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=459
Status	New

The function nm in freebsd-src-3/t_regex_att.c at line 383 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	freebsd-src-3/t_regex_att.c	freebsd-src-3/t_regex_att.c
Line	492	492
Object	nm	nm

Code Snippet
File Name freebsd-src-3/t_regex_att.c
Method att_test(const struct atf_tc *tc, const char *data_name)

```
....
492.                    ATF_REQUIRE((pm = calloc(nm, sizeof(*pm))) !=
NULL);
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=997
Status	New

The variable declared in ifp at freebsd-src-3/icmp6.c in line 1673 is not initialized when it is used by ifp at freebsd-src-3/icmp6.c in line 1673.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1676	1752

Object	ifp	ifp

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_addrs(struct icmp6_nodeinfo *ni6, struct mbuf *m, struct ifnet **ifpp,

```
....
1676.        struct ifnet *ifp;
....
1752.                     *ifpp = ifp;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=998
Status	New

The variable declared in nip6 at freebsd-src-3/icmp6.c in line 256 is not initialized when it is used by ip6_dst at freebsd-src-3/icmp6.c in line 256.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	258	369
Object	nip6	ip6_dst

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_error(struct mbuf *m, int type, int code, int param)

```
....
258.         struct ip6_hdr *oip6, *nip6;
....
369.         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=1060099&projectid=60089&pathid=999
Status	New

The variable declared in nip6 at freebsd-src-3/icmp6.c in line 256 is not initialized when it is used by ip6_src at freebsd-src-3/icmp6.c in line 256.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c

Line	258	368
Object	nip6	ip6_src

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_error(struct mbuf *m, int type, int code, int param)

```
....
258.        struct ip6_hdr *oip6, *nip6;
....
368.        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=1060099&projectid=60089&pathid=1000
Status New

The variable declared in nip6 at freebsd-src-3/icmp6.c in line 256 is not initialized when it is used by nip6 at freebsd-src-3/icmp6.c in line 256.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	258	374
Object	nip6	nip6

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_error(struct mbuf *m, int type, int code, int param)

```
....
258.        struct ip6_hdr *oip6, *nip6;
....
374.        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=1060099&projectid=60089&pathid=1001
Status New

The variable declared in ifa at freebsd-src-3/icmp6.c in line 1673 is not initialized when it is used by ifa at freebsd-src-3/icmp6.c in line 1673.

	Source	Destination

File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1678	1704
Object	ifa	ifa

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_addrs(struct icmp6_nodeinfo *ni6, struct mbuf *m, struct ifnet **ifpp,

```
....
1678.       struct ifaddr *ifa;
....
1704.                   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=1060099&projectid=60089&pathid=1002
Status	New

The variable declared in ifa at freebsd-src-3/icmp6.c in line 1673 is not initialized when it is used by ifa_addr at freebsd-src-3/icmp6.c in line 1673.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1678	1702
Object	ifa	ifa_addr

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_addrs(struct icmp6_nodeinfo *ni6, struct mbuf *m, struct ifnet **ifpp,

```
....
1678.       struct ifaddr *ifa;
....
1702.                   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=1060099&projectid=60089&pathid=1003
Status	New

The variable declared in ifa at freebsd-src-3/icmp6.c in line 1763 is not initialized when it is used by ifa at freebsd-src-3/icmp6.c in line 1763.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1768	1787
Object	ifa	ifa

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1768.       struct ifaddr *ifa;
....
1787.                   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=1060099&projectid=60089&pathid=1004
Status New

The variable declared in ifa at freebsd-src-3/icmp6.c in line 1763 is not initialized when it is used by ifa_addr at freebsd-src-3/icmp6.c in line 1763.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1768	1785
Object	ifa	ifa_addr

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1768.       struct ifaddr *ifa;
....
1785.                   if (ifa->ifa_addr->sa_family != AF_INET6)
```

Use of Uninitialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1005
Status New

The variable declared in bf at freebsd-src-3/if_mwl.c in line 3519 is not initialized when it is used by bf at freebsd-src-3/if_mwl.c in line 3519.

	Source	Destination
File	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c
Line	3522	3531
Object	bf	bf

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_cleartxq(struct mwl_softc *sc, struct ieee80211vap *vap)

```
....
3522.        struct mwl_txbuf *bf;
....
3531.                            bf->bf_node = NULL;
```

Use of Uninitialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1006
Status New

The variable declared in bf at freebsd-src-3/if_mwl.c in line 3519 is not initialized when it is used by bf_node at freebsd-src-3/if_mwl.c in line 3519.

	Source	Destination
File	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c
Line	3522	3529
Object	bf	bf_node

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_cleartxq(struct mwl_softc *sc, struct ieee80211vap *vap)

```
....
3522.        struct mwl_txbuf *bf;
....
3529.                    struct ieee80211_node *ni = bf->bf_node;
```

Buffer Overflow Loops

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow Loops\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=438
Status	New

The buffer allocated by offset in freebsd-src-3/chksum.c at line 168 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	280	333
Object	0	offset

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
280.      uint8_t *base = mmap(0, POOLSIZE, PROT_READ|PROT_WRITE,
....
333.            success &= verify(&base[offset], offset, size);
```

Buffer Overflow Loops\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=439
Status	New

The buffer allocated by i in freebsd-src-3/chksum.c at line 168 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	280	318
Object	0	i

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
280.      uint8_t *base = mmap(0, POOLSIZE, PROT_READ|PROT_WRITE,
....
318.            printf(" %02x", base[i]);
```

Buffer Overflow Loops\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=440
Status	New

The buffer allocated by offset in freebsd-src-3/chksum.c at line 168 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	281	333
Object	0	offset

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
281.                    MAP_PRIVATE|MAP_ANONYMOUS, -1, 0);
....
333.            success &= verify(&base[offset], offset, size);
```

Buffer Overflow Loops\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=441
Status	New

The buffer allocated by i in freebsd-src-3/chksum.c at line 168 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	281	318
Object	0	i

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
281.                    MAP_PRIVATE|MAP_ANONYMOUS, -1, 0);
....
318.            printf(" %02x", base[i]);
```

Buffer Overflow Loops\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=442
Status	New

The buffer allocated by offset in freebsd-src-3/chksum.c at line 168 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	281	333
Object	-1	offset

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
281.                    MAP_PRIVATE|MAP_ANONYMOUS, -1, 0);
....
333.            success &= verify(&base[offset], offset, size);
```

Buffer Overflow Loops\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=443
Status	New

The buffer allocated by i in freebsd-src-3/chksum.c at line 168 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	281	318
Object	-1	i

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
281.                    MAP_PRIVATE|MAP_ANONYMOUS, -1, 0);
....
318.            printf(" %02x", base[i]);
```

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=1060099&projectid=60089&pathid=460
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 319 of freebsd-src-3/fetch.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c
Line	328	328
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetch_pctdecode(char *dst, const char *src, size_t dlen)

```
....
328.                    c = d1 << 4 | d2;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=461
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 327 of freebsd-src-3/test_write_format_iso9660_zisofs.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/test_write_format_iso9660_zisofs.c	freebsd-src-3/test_write_format_iso9660_zisofs.c
Line	375	375
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/test_write_format_iso9660_zisofs.c

Method	test_write_format_iso9660_zisofs_2(void)

```
....
375.                                data[j] = (i^j) & 0xff;
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=462
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 327 of freebsd-src-3/test_write_format_iso9660_zisofs.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/test_write_format_iso9660_zisofs.c	freebsd-src-3/test_write_format_iso9660_zisofs.c
Line	378	378
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	freebsd-src-3/test_write_format_iso9660_zisofs.c
Method	test_write_format_iso9660_zisofs_2(void)

```
....
378.                                data[j] ^= i+j;
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=915
Status	New

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	916	923
Object	str	str

Code Snippet
File Name freebsd-src-3/print.c
Method hx509_validate_cert(hx509_context context,

```
....
916.        free(str);
....
923.        free(str);
```

Double Free\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=916
Status New

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	923	936
Object	str	str

Code Snippet
File Name freebsd-src-3/print.c
Method hx509_validate_cert(hx509_context context,

```
....
923.        free(str);
....
936.        free(str);
```

Double Free\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=917
Status New

	Source	Destination
File	freebsd-src-3/print.c	freebsd-src-3/print.c
Line	936	939
Object	str	str

Code Snippet
File Name freebsd-src-3/print.c
Method hx509_validate_cert(hx509_context context,

```
....
936.        free(str);
....
939.        free(str);
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=919
Status	New

Method eap_get_ext_password at line 2778 of freebsd-src-3/eap.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	2782	2782
Object	password	password

Code Snippet
File Name freebsd-src-3/eap.c
Method static int eap_get_ext_password(struct eap_sm *sm,

```
....
2782.        const u8 *password;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=920
Status	New

Method eap_get_ext_password at line 2778 of freebsd-src-3/eap.c defines password_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_len, this variable is never cleared from memory.

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	2783	2783
Object	password_len	password_len

Code Snippet
File Name freebsd-src-3/eap.c
Method static int eap_get_ext_password(struct eap_sm *sm,

```
....
2783.       size_t password_len;
```

Inadequate Encryption Strength

Query Path:
CPP\Cx\CPP Medium Threat\Inadequate Encryption Strength Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-13 Cryptographic Protection (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description
Inadequate Encryption Strength\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1007
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 893 of freebsd-src-3/print-tcp.c, to protect sensitive personal information ndo_sigsecret, from freebsd-src-3/print-tcp.c at line 893.

	Source	Destination
File	freebsd-src-3/print-tcp.c	freebsd-src-3/print-tcp.c
Line	963	963
Object	ndo_sigsecret	MD5_Update

Code Snippet
File Name freebsd-src-3/print-tcp.c
Method tcp_verify_signature(netdissect_options *ndo,

```
....
963.          MD5_Update(&ctx, ndo->ndo_sigsecret, strlen(ndo-
>ndo_sigsecret));
```

Inadequate Encryption Strength\Path 2:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1008
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 893 of freebsd-src-3/print-tcp.c, to protect sensitive personal information ndo_sigsecret, from freebsd-src-3/print-tcp.c at line 893.

	Source	Destination
File	freebsd-src-3/print-tcp.c	freebsd-src-3/print-tcp.c
Line	963	963
Object	ndo_sigsecret	MD5_Update

Code Snippet
File Name freebsd-src-3/print-tcp.c
Method tcp_verify_signature(netdissect_options *ndo,

```
....
963.          MD5_Update(&ctx, ndo->ndo_sigsecret, strlen(ndo-
>ndo_sigsecret));
```

Use of a One Way Hash without a Salt

Query Path:
CPP\Cx\CPP Medium Threat\Use of a One Way Hash without a Salt Version:1

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-13 Cryptographic Protection (P1)

Description
Use of a One Way Hash without a Salt\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1009
Status	New

The application protects passwords with SHA1_Final in aesni_cbc_hmac_sha1_ctrl, of freebsd-src-3/e_aes_cbc_hmac_sha1.c at line 768, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	782	784
Object	Address	SHA1_Final

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```
....
782.                    SHA1_Init(&key->head);
....
784.                    SHA1_Final(hmac_key, &key->head);
```

Use of a One Way Hash without a Salt\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1010
Status	New

The application protects passwords with SHA256_Final in aesni_cbc_hmac_sha256_ctrl, of freebsd-src-3/e_aes_cbc_hmac_sha256.c at line 745, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	763	765
Object	Address	SHA256_Final

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```
....
763.                    SHA256_Init(&key->head);
....
765.                    SHA256_Final(hmac_key, &key->head);
```

Wrong Memory Allocation

Query Path:
CPP\Cx\CPP Medium Threat\Wrong Memory Allocation Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Wrong Memory Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1556
Status	New

The function malloc in freebsd-src-3/addrtoname.c at line 705 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	719	719
Object	sizeof	malloc

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method isonsap_string(netdissect_options *ndo, const uint8_t *nsap,

```
....
719.        tp->e_name = cp = (char
*)malloc(sizeof("xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx"));
```

Wrong Memory Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1557
Status	New

The function malloc in freebsd-src-3/pst-iop.c at line 63 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	freebsd-src-3/pst-iop.c	freebsd-src-3/pst-iop.c
Line	89	89
Object	sizeof	malloc

Code Snippet
File Name freebsd-src-3/pst-iop.c
Method iop_init(struct iop_softc *sc)

```
....
89.                         malloc(sizeof(struct intr_config_hook),
```

Short Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Short Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Short Overflow\Path 1:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=490
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1910 of freebsd-src-3/ssl3_record.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c
Line	1969	1969
Object	AssignExpr	AssignExpr

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method int dtls1_get_record(SSL *s)

```
....
1969.           version = (ssl_major << 8) | ssl_minor;
```

Use of Hard coded Cryptographic Key

Query Path:
CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Hard coded Cryptographic Key\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=918
Status	New

The variable keyEncipherment at line 406 of freebsd-src-3/check-gen.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	freebsd-src-3/check-gen.c	freebsd-src-3/check-gen.c
Line	436	436
Object	keyEncipherment	keyEncipherment

Code Snippet
File Name freebsd-src-3/check-gen.c
Method test_bit_string (void)

```
....
436.      ku2.keyEncipherment = 1;
```

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=1060099&projectid=60089&pathid=1030
Status	New

The LoadValueFromConsecutiveGPRRegisters method calls the snprintf function, at line 490 of freebsd-src-3/ABIMacOSX_arm64.cpp. 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	freebsd-src-3/ABIMacOSX_arm64.cpp	freebsd-src-3/ABIMacOSX_arm64.cpp
Line	523	523
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/ABIMacOSX_arm64.cpp
Method static bool LoadValueFromConsecutiveGPRRegisters(

```
....
523.          ::snprintf(v_name, sizeof(v_name), "v%u", NSRN);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1031
Status	New

The ieee8021q_tci_string method calls the snprintf function, at line 1322 of freebsd-src-3/addrtoname.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	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c

Line	1325	1325
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method ieee8021q_tci_string(const uint16_t tci)

```
....
1325.       snprintf(buf, sizeof(buf), "vlan %u, p %u%s",
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1032
Status	New

The etheraddr_string method calls the snprintf function, at line 588 of freebsd-src-3/addrtoname.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	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	628	628
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method etheraddr_string(netdissect_options *ndo, const uint8_t *ep)

```
....
628.              snprintf(cp, BUFSIZE - (2 + 5*3), " (oui %s)",
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1033
Status	New

The tcpport_string method calls the snprintf function, at line 736 of freebsd-src-3/addrtoname.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	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c

Line	749	749
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method tcpport_string(netdissect_options *ndo, u_short port)

```
....
749.         (void)snprintf(buf, sizeof(buf), "%u", i);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1034
Status	New

The udpport_string method calls the snprintf function, at line 758 of freebsd-src-3/addrtoname.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	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	771	771
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method udpport_string(netdissect_options *ndo, u_short port)

```
....
771.         (void)snprintf(buf, sizeof(buf), "%u", i);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1035
Status	New

The init_servarray method calls the snprintf function, at line 809 of freebsd-src-3/addrtoname.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	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c

Line	829	829
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method init_servarray(netdissect_options *ndo)

```
....
829.                    (void)snprintf(buf, sizeof(buf), "%d", port);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1036
Status	New

The es256_sk_new method calls the calloc function, at line 135 of freebsd-src-3/es256.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	freebsd-src-3/es256.c	freebsd-src-3/es256.c
Line	137	137
Object	calloc	calloc

Code Snippet
File Name freebsd-src-3/es256.c
Method es256_sk_new(void)

```
....
137.        return (calloc(1, sizeof(es256_sk_t)));
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1037
Status	New

The es256_pk_new method calls the calloc function, at line 153 of freebsd-src-3/es256.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	freebsd-src-3/es256.c	freebsd-src-3/es256.c

Line	155	155
Object	calloc	calloc

Code Snippet
File Name freebsd-src-3/es256.c
Method es256_pk_new(void)

```
....
155.        return (calloc(1, sizeof(es256_pk_t)));
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1038
Status New

The fdt_pinctrl_configure method calls the snprintf function, at line 41 of freebsd-src-3/fdt_pinctrl.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	freebsd-src-3/fdt_pinctrl.c	freebsd-src-3/fdt_pinctrl.c
Line	48	48
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/fdt_pinctrl.c
Method fdt_pinctrl_configure(device_t client, u_int index)

```
....
48.    snprintf(name, sizeof(name), "pinctrl-%u", index);
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1039
Status New

The fetchMakeURL method calls the snprintf function, at line 257 of freebsd-src-3/fetch.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	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c

Line	286	286
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetchMakeURL(const char *scheme, const char *host, int port, const char *doc,

```
....
286.        seturl(scheme);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1040
Status	New

The fetchMakeURL method calls the snprintf function, at line 257 of freebsd-src-3/fetch.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	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c
Line	287	287
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetchMakeURL(const char *scheme, const char *host, int port, const char *doc,

```
....
287.        seturl(host);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1041
Status	New

The fetchMakeURL method calls the snprintf function, at line 257 of freebsd-src-3/fetch.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	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c

Line	288	288
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetchMakeURL(const char *scheme, const char *host, int port, const char *doc,

```
....
288.        seturl(user);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1042
Status	New

The fetchMakeURL method calls the snprintf function, at line 257 of freebsd-src-3/fetch.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	freebsd-src-3/fetch.c	freebsd-src-3/fetch.c
Line	289	289
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/fetch.c
Method fetchMakeURL(const char *scheme, const char *host, int port, const char *doc,

```
....
289.        seturl(pwd);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1043
Status	New

The hostapd_cli_cmd_sta method calls the snprintf function, at line 310 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	319	319
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_sta(struct wpa_ctrl *ctrl, int argc, char *argv[])

```
....
319.                snprintf(buf, sizeof(buf), "STA %s %s", argv[0],
argv[1]);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1044
Status	New

The hostapd_cli_cmd_sta method calls the snprintf function, at line 310 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	321	321
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_sta(struct wpa_ctrl *ctrl, int argc, char *argv[])

```
....
321.                snprintf(buf, sizeof(buf), "STA %s", argv[0]);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1045
Status	New

The hostapd_cli_cmd_new_sta method calls the snprintf function, at line 341 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	350	350
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_new_sta(struct wpa_ctrl *ctrl, int argc,

```
....
350.        snprintf(buf, sizeof(buf), "NEW_STA %s", argv[0]);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1046
Status	New

The hostapd_cli_cmd_sa_query method calls the snprintf function, at line 407 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	416	416
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_sa_query(struct wpa_ctrl *ctrl, int argc,

```
....
416.        snprintf(buf, sizeof(buf), "SA_QUERY %s", argv[0]);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1047
Status	New

The hostapd_cli_cmd_wps_pin method calls the snprintf function, at line 422 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	432	432
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_pin(struct wpa_ctrl *ctrl, int argc,

```
....
432.             snprintf(buf, sizeof(buf), "WPS_PIN %s %s %s %s",
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1048
Status	New

The hostapd_cli_cmd_wps_pin method calls the snprintf function, at line 422 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	435	435
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_pin(struct wpa_ctrl *ctrl, int argc,

```
....
435.             snprintf(buf, sizeof(buf), "WPS_PIN %s %s %s",
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1049
Status	New

The hostapd_cli_cmd_wps_pin method calls the snprintf function, at line 422 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	438	438
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_pin(struct wpa_ctrl *ctrl, int argc,

```
....
438.                snprintf(buf, sizeof(buf), "WPS_PIN %s %s", argv[0],
argv[1]);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1050
Status	New

The hostapd_cli_cmd_wps_ap_pin method calls the snprintf function, at line 577 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	587	587
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_ap_pin(struct wpa_ctrl *ctrl, int argc,

```
....
587.                snprintf(buf, sizeof(buf), "WPS_AP_PIN %s %s %s",
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1051
Status	New

The hostapd_cli_cmd_wps_ap_pin method calls the snprintf function, at line 577 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	590	590
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_ap_pin(struct wpa_ctrl *ctrl, int argc,

```
....
590.            snprintf(buf, sizeof(buf), "WPS_AP_PIN %s %s",
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1052
Status	New

The hostapd_cli_cmd_wps_ap_pin method calls the snprintf function, at line 577 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	593	593
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_ap_pin(struct wpa_ctrl *ctrl, int argc,

```
....
593.            snprintf(buf, sizeof(buf), "WPS_AP_PIN %s", argv[0]);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1053
Status	New

The hostapd_cli_cmd_wps_config method calls the snprintf function, at line 605 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	637	637
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_config(struct wpa_ctrl *ctrl, int argc,

```
....
637.                snprintf(buf, sizeof(buf), "WPS_CONFIG %s %s %s %s",
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1054
Status	New

The hostapd_cli_cmd_wps_config method calls the snprintf function, at line 605 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	640	640
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_config(struct wpa_ctrl *ctrl, int argc,

```
....
640.                snprintf(buf, sizeof(buf), "WPS_CONFIG %s %s %s",
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1055
Status	New

The hostapd_cli_cmd_wps_config method calls the snprintf function, at line 605 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	643	643
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_wps_config(struct wpa_ctrl *ctrl, int argc,

```
....
643.                snprintf(buf, sizeof(buf), "WPS_CONFIG %s %s",
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1056
Status	New

The hostapd_cli_cmd_all_sta method calls the snprintf function, at line 761 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	769	769
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_all_sta(struct wpa_ctrl *ctrl, int argc,

```
....
769.                snprintf(cmd, sizeof(cmd), "STA-NEXT %s", addr);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1057
Status	New

The hostapd_cli_cmd_level method calls the snprintf function, at line 916 of freebsd-src-3/hostapd_cli.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	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	924	924
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_level(struct wpa_ctrl *ctrl, int argc, char *argv[])

```
....
924.        snprintf(cmd, sizeof(cmd), "LEVEL %s", argv[0]);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1058
Status	New

The *ath10k_get_tid method calls the snprintf function, at line 1339 of freebsd-src-3/htt_rx.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	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	1350	1350
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static char *ath10k_get_tid(struct ieee80211_hdr *hdr, char *out, size_t size)

```
....
1350.             snprintf(out, size, "tid %d (%s)", tid,
tid_to_ac[tid]);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1059
Status	New

The *ath10k_get_tid method calls the snprintf function, at line 1339 of freebsd-src-3/htt_rx.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	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c

Line	1352	1352
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static char *ath10k_get_tid(struct ieee80211_hdr *hdr, char *out, size_t size)

```
....
1352.             snprintf(out, size, "tid %d", tid);
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1060
Status New

The main method calls the _snprintf function, at line 215 of freebsd-src-3/https-client.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	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	336	336
Object	_snprintf	_snprintf

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
336.             snprintf(uri, sizeof(uri) - 1, "%s", path);
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1061
Status New

The main method calls the _snprintf function, at line 215 of freebsd-src-3/https-client.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	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c

Line	338	338
Object	_snprintf	_snprintf

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
338.              snprintf(uri, sizeof(uri) - 1, "%s?%s", path, query);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1062
Status	New

The icmp6_redirect_diag method calls the snprintf function, at line 2151 of freebsd-src-3/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	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2158	2158
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_diag(struct in6_addr *src6, struct in6_addr *dst6,

```
....
2158.       snprintf(buf, sizeof(buf), "(src=%s dst=%s tgt=%s)",
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1063
Status	New

The ti_sysctl_node method calls the snprintf function, at line 3975 of freebsd-src-3/if_ti.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	freebsd-src-3/if_ti.c	freebsd-src-3/if_ti.c

Line	3986	3986
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/if_ti.c
Method ti_sysctl_node(struct ti_softc *sc)

```
....
3986.       snprintf(tname, sizeof(tname), "dev.ti.%d.dac",
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1064
Status	New

The ldns_rdf_reverse_a method calls the sprintf function, at line 88 of freebsd-src-3/ldns-host.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	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	97	97
Object	sprintf	sprintf

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_rdf_reverse_a(ldns_rdf *addr, const char *base) {

```
....
97.      sprintf(&buf[len], "%s", base);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1065
Status	New

The ldns_rdf_reverse_aaaa method calls the sprintf function, at line 102 of freebsd-src-3/ldns-host.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	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c

Line	110	110
Object	sprintf	sprintf

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_rdf_reverse_aaaa(ldns_rdf *addr, const char *base) {

```
....
110.          sprintf(&buf[i*4], "%x.%x.", byte & 0x0F, byte >> 4);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1066
Status	New

The ldns_rdf_reverse_aaaa method calls the sprintf function, at line 102 of freebsd-src-3/ldns-host.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	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	112	112
Object	sprintf	sprintf

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_rdf_reverse_aaaa(ldns_rdf *addr, const char *base) {

```
....
112.      sprintf(&buf[LDNS_IP6ADDRLEN*4], "%s", base);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1067
Status	New

The mmc_format_card_id_string method calls the snprintf function, at line 402 of freebsd-src-3/mmc_da.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	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c

Line	427	427
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method mmc_format_card_id_string(struct sdda_softc *sc, struct mmc_params *mmcp)

```
....
427.              snprintf(oidstr, sizeof(oidstr), "%c%c", c1, c2);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1068
Status	New

The mmc_format_card_id_string method calls the snprintf function, at line 402 of freebsd-src-3/mmc_da.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	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c
Line	429	429
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method mmc_format_card_id_string(struct sdda_softc *sc, struct mmc_params *mmcp)

```
....
429.              snprintf(oidstr, sizeof(oidstr), "0x%04x", sc-
>cid.oid);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1069
Status	New

The mmc_format_card_id_string method calls the snprintf function, at line 402 of freebsd-src-3/mmc_da.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	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c

Line	430	430
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method mmc_format_card_id_string(struct sdda_softc *sc, struct mmc_params *mmcp)

```
....
430.        snprintf(sc->card_sn_string, sizeof(sc->card_sn_string),
```

Unchecked Return Value\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1070
Status New

The mmc_format_card_id_string method calls the snprintf function, at line 402 of freebsd-src-3/mmc_da.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	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c
Line	432	432
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method mmc_format_card_id_string(struct sdda_softc *sc, struct mmc_params *mmcp)

```
....
432.        snprintf(sc->card_id_string, sizeof(sc->card_id_string),
```

Unchecked Return Value\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1071
Status New

The sdda_add_part method calls the snprintf function, at line 1507 of freebsd-src-3/mmc_da.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	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c

Line	1531	1531
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method sdda_add_part(struct cam_periph *periph, u_int type, const char *name,

```
....
1531.       snprintf(part->name, sizeof(part->name), name, periph-
>unit_number);
```

Unchecked Return Value\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1072
Status New

The sdda_add_part method calls the snprintf function, at line 1507 of freebsd-src-3/mmc_da.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	freebsd-src-3/mmc_da.c	freebsd-src-3/mmc_da.c
Line	1589	1589
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/mmc_da.c
Method sdda_add_part(struct cam_periph *periph, u_int type, const char *name,

```
....
1589.       snprintf(part->disk->d_attachment, sizeof(part->disk-
>d_attachment),
```

Unchecked Return Value\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1073
Status New

The parse_dsserver method calls the snprintf function, at line 1179 of freebsd-src-3/nfsd.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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1219	1219
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1219.       snprintf(nfsprt, 9, ".%d.%d", 2049 >> 8, 2049 & 0xff);
```

Unchecked Return Value\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1074
Status New

The start_server method calls the snprintf function, at line 1019 of freebsd-src-3/nfsd.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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1031	1031
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/nfsd.c
Method start_server(int master, struct nfsd_nfsd_args *nfsdargp, const char *vhost)

```
....
1031.       snprintf(principal, sizeof (principal), "nfs@%s", hostname);
```

Unchecked Return Value\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1075
Status New

The start_server method calls the snprintf function, at line 1019 of freebsd-src-3/nfsd.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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1042	1042
Object	snprintf	snprintf

Code Snippet
File Name freebsd-src-3/nfsd.c
Method start_server(int master, struct nfsd_nfsd_args *nfsdargp, const char *vhost)

```
....
1042.                          snprintf(principal, sizeof (principal),
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1076
Status	New

The main method calls the sprintf function, at line 2928 of freebsd-src-3/pkt-gen.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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	3058	3058
Object	sprintf	sprintf

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method main(int arc, char **argv)

```
....
3058.                          sprintf(g.ifname, "netmap:%s", optarg);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1077
Status	New

The source_hwaddr method calls the sprintf function, at line 679 of freebsd-src-3/pkt-gen.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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c

Line	702	702
Object	sprintf	sprintf

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method source_hwaddr(const char *ifname, char *buf)

```
....
702.                sprintf(buf, "%02x:%02x:%02x:%02x:%02x:%02x",
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1078
Status	New

The dump_payload method calls the sprintf function, at line 772 of freebsd-src-3/pkt-gen.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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	786	786
Object	sprintf	sprintf

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method dump_payload(const char *_p, int len, struct netmap_ring *ring, int cur)

```
....
786.                sprintf(buf, "%5d: ", i);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1079
Status	New

The dump_payload method calls the sprintf function, at line 772 of freebsd-src-3/pkt-gen.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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c

Line	789	789
Object	sprintf	sprintf

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method dump_payload(const char *_p, int len, struct netmap_ring *ring, int cur)

```
....
789.                    sprintf(buf+7+j*3, "%02x ", (uint8_t)(p[i]));
```

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=1060099&projectid=60089&pathid=1706
Status New

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	462	462
Object	realm_len	realm_len

Code Snippet
File Name freebsd-src-3/eap.c
Method static char * eap_get_realm(struct eap_sm *sm, struct eap_peer_config *config)

```
....
462.                    realm[realm_len] = '\0';
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1707
Status New

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c

Line	479	479
Object	realm_len	realm_len

Code Snippet
File Name freebsd-src-3/eap.c
Method static char * eap_get_realm(struct eap_sm *sm, struct eap_peer_config *config)

```
....
479.                    realm[realm_len] = '\0';
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1708
Status New

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	761	761
Object	pos	pos

Code Snippet
File Name freebsd-src-3/eap.c
Method void eap_peer_erp_init(struct eap_sm *sm, u8 *ext_session_id,

```
....
761.        erp->keyname_nai[pos] = '@';
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1709
Status New

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	1984	1984
Object	RETVAL_LO	RETVAL_LO

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_lseek(struct thread *td, struct freebsd32_lseek_args *uap)

```
....
1984.       td->td_retval[RETVAL_LO] = pos & 0xffffffff;    /* %eax */
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1710
Status	New

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	1985	1985
Object	RETVAL_HI	RETVAL_HI

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_lseek(struct thread *td, struct freebsd32_lseek_args *uap)

```
....
1985.       td->td_retval[RETVAL_HI] = pos >> 32;           /* %edx */
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1711
Status	New

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	2090	2090
Object	RETVAL_LO	RETVAL_LO

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd6_freebsd32_lseek(struct thread *td, struct freebsd6_freebsd32_lseek_args *uap)

```
....
2090.       td->td_retval[RETVAL_LO] = pos & 0xffffffff;    /* %eax */
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1712
Status	New

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	2091	2091
Object	RETVAL_HI	RETVAL_HI

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd6_freebsd32_lseek(struct thread *td, struct freebsd6_freebsd32_lseek_args *uap)

```
....
2091.       td->td_retval[RETVAL_HI] = pos >> 32;           /* %edx */
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1713
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	214	214
Object	len	len

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int _wpa_ctrl_command(struct wpa_ctrl *ctrl, const char *cmd, int print)

```
....
214.              buf[len] = '\0';
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1714
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c

Line	746	746
Object	len	len

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int wpa_ctrl_command_sta(struct wpa_ctrl *ctrl, const char *cmd,

```
....
746.        buf[len] = '\0';
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1715
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	103	103
Object	idx	idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static void ath10k_htt_set_paddrs_ring_32(struct ath10k_htt *htt,

```
....
103.        htt->rx_ring.paddrs_ring_32[idx] = __cpu_to_le32(paddr);
```

Unchecked Array Index\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1716
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	109	109
Object	idx	idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static void ath10k_htt_set_paddrs_ring_64(struct ath10k_htt *htt,

```
....
109.        htt->rx_ring.paddrs_ring_64[idx] = __cpu_to_le64(paddr);
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1717
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	114	114
Object	idx	idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static void ath10k_htt_reset_paddrs_ring_32(struct ath10k_htt *htt, int idx)

```
....
114.        htt->rx_ring.paddrs_ring_32[idx] = 0;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1718
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	119	119
Object	idx	idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static void ath10k_htt_reset_paddrs_ring_64(struct ath10k_htt *htt, int idx)

```
....
119.        htt->rx_ring.paddrs_ring_64[idx] = 0;
```

Unchecked Array Index\Path 14:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1719
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	327	327
Object	idx	idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static inline struct sk_buff *ath10k_htt_rx_netbuf_pop(struct ath10k_htt *htt)

```
....
327.        htt->rx_ring.netbufs_ring[idx] = NULL;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1720
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	2580	2580
Object	tid	tid

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method static bool ath10k_htt_rx_pn_check_replay_hl(struct ath10k *ar,

```
....
2580.            peer->tids_last_pn_valid[tid] = true;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1721
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3832	3832

Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3832.              STATS_OP_FMT(SUCC).vht[0][mcs] += pstats->succ_bytes;
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1722
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3833	3833
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3833.              STATS_OP_FMT(SUCC).vht[1][mcs] += pstats->succ_pkts;
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1723
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3834	3834
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3834.             STATS_OP_FMT(FAIL).vht[0][mcs] += pstats-
>failed_bytes;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1724
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3835	3835
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3835.             STATS_OP_FMT(FAIL).vht[1][mcs] += pstats->failed_pkts;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1725
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3836	3836
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3836.             STATS_OP_FMT(RETRY).vht[0][mcs] += pstats-
>retry_bytes;
```

Unchecked Array Index\Path 21:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1726
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3837	3837
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3837.             STATS_OP_FMT(RETRY).vht[1][mcs] += pstats->retry_pkts;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1727
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3839	3839
Object	ht_idx	ht_idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3839.             STATS_OP_FMT(SUCC).ht[0][ht_idx] += pstats-
>succ_bytes;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1728
Status	New

	Source	Destination

File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3840	3840
Object	ht_idx	ht_idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3840.             STATS_OP_FMT(SUCC).ht[1][ht_idx] += pstats->succ_pkts;
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1729
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3841	3841
Object	ht_idx	ht_idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3841.             STATS_OP_FMT(FAIL).ht[0][ht_idx] += pstats-
>failed_bytes;
```

Unchecked Array Index\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1730
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3842	3842
Object	ht_idx	ht_idx

Code Snippet
File Name freebsd-src-3/htt_rx.c

Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3842.              STATS_OP_FMT(FAIL).ht[1][ht_idx] += pstats-
>failed_pkts;
```

Unchecked Array Index\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1731
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3843	3843
Object	ht_idx	ht_idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3843.              STATS_OP_FMT(RETRY).ht[0][ht_idx] += pstats-
>retry_bytes;
```

Unchecked Array Index\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1732
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3844	3844
Object	ht_idx	ht_idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3844.              STATS_OP_FMT(RETRY).ht[1][ht_idx] += pstats-
>retry_pkts;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1733
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3848	3848
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3848.              STATS_OP_FMT(SUCC).legacy[0][mcs] += pstats-
>succ_bytes;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1734
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3849	3849
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3849.              STATS_OP_FMT(SUCC).legacy[1][mcs] += pstats-
>succ_pkts;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1735
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3850	3850
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3850.              STATS_OP_FMT(FAIL).legacy[0][mcs] += pstats-
>failed_bytes;
```

Unchecked Array Index\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1736
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3851	3851
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3851.              STATS_OP_FMT(FAIL).legacy[1][mcs] += pstats-
>failed_pkts;
```

Unchecked Array Index\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1737
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3852	3852
Object	mcs	mcs

Code Snippet	
File Name	freebsd-src-3/htt_rx.c
Method	ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3852.              STATS_OP_FMT(RETRY).legacy[0][mcs] += pstats-
>retry_bytes;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1738
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3853	3853
Object	mcs	mcs

Code Snippet	
File Name	freebsd-src-3/htt_rx.c
Method	ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3853.              STATS_OP_FMT(RETRY).legacy[1][mcs] += pstats-
>retry_pkts;
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1739
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3860	3860
Object	ht_idx	ht_idx

Code Snippet	
File Name	freebsd-src-3/htt_rx.c
Method	ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3860.                    STATS_OP_FMT(AMPDU).ht[0][ht_idx] +=
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1740
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3862	3862
Object	ht_idx	ht_idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3862.                    STATS_OP_FMT(AMPDU).ht[1][ht_idx] +=
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1741
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3865	3865
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3865.                    STATS_OP_FMT(AMPDU).vht[0][mcs] +=
```

Unchecked Array Index\Path 37:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1742
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3867	3867
Object	mcs	mcs

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3867.                    STATS_OP_FMT(AMPDU).vht[1][mcs] +=
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1743
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3870	3870
Object	bw	bw

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3870.              STATS_OP_FMT(AMPDU).bw[0][bw] +=
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1744
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3874	3874

Object	gi	gi

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3874.              STATS_OP_FMT(AMPDU).gi[0][gi] +=
```

Unchecked Array Index\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1745
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3876	3876
Object	idx	idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3876.              STATS_OP_FMT(AMPDU).rate_table[0][idx] +=
```

Unchecked Array Index\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1746
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3878	3878
Object	bw	bw

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3878.              STATS_OP_FMT(AMPDU).bw[1][bw] +=
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1747
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3882	3882
Object	gi	gi

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3882.              STATS_OP_FMT(AMPDU).gi[1][gi] +=
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1748
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3884	3884
Object	idx	idx

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3884.              STATS_OP_FMT(AMPDU).rate_table[1][idx] +=
```

Unchecked Array Index\Path 44:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1749
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3891	3891
Object	bw	bw

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3891.        STATS_OP_FMT(SUCC).bw[0][bw] += pstats->succ_bytes;
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1750
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3893	3893
Object	gi	gi

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3893.        STATS_OP_FMT(SUCC).gi[0][gi] += pstats->succ_bytes;
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1751
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3895	3895

Object	bw	bw

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3895.        STATS_OP_FMT(SUCC).bw[1][bw] += pstats->succ_pkts;
```

Unchecked Array Index\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1752
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3897	3897
Object	gi	gi

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3897.        STATS_OP_FMT(SUCC).gi[1][gi] += pstats->succ_pkts;
```

Unchecked Array Index\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1753
Status New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3899	3899
Object	bw	bw

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3899.       STATS_OP_FMT(FAIL).bw[0][bw] += pstats->failed_bytes;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1754
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3901	3901
Object	gi	gi

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3901.       STATS_OP_FMT(FAIL).gi[0][gi] += pstats->failed_bytes;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1755
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3903	3903
Object	bw	bw

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_accumulate_per_peer_tx_stats(struct ath10k *ar,

```
....
3903.       STATS_OP_FMT(FAIL).bw[1][bw] += pstats->failed_pkts;
```

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=1060099&projectid=60089&pathid=1228
Status	New

The variable declared in null at freebsd-src-3/eap.c in line 684 is not initialized when it is used by erp at freebsd-src-3/eap.c in line 684.

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	787	794
Object	null	erp

Code Snippet
File Name freebsd-src-3/eap.c
Method void eap_peer_erp_init(struct eap_sm *sm, u8 *ext_session_id,

```
....
787.        erp = NULL;
....
794.        bin_clear_free(erp, sizeof(*erp));
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1229
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	881	255
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
881.          FillAdOfTypeContLookup(h_Ad, NULL, p_CcNode->h_FmPcd,
p_FmPcdCcNodeTmp,
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1230
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	890	255
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static t_Handle BuildNewAd(

```
....
890.                  h_Ad, NULL, p_CcNode->h_FmPcd, p_FmPcdCcNodeTmp,
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1231
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 377 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	403	255
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/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 freebsd-src-3/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1232
Status New

The variable declared in null at freebsd-src-3/fm_cc.c in line 2566 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	2686	255
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2686.                  NextStepAd(p_AdTableNewTmp, NULL,
```

File Name	freebsd-src-3/fm_cc.c
Method	static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1233
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5994 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	6197	255
Object	null	h_StatsFLRs

Code Snippet

File Name	freebsd-src-3/fm_cc.c
Method	t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6197.          NextStepAd(p_CcTreeTmp, NULL,
```

File Name	freebsd-src-3/fm_cc.c
Method	static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1234
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination

File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4815	255
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error MatchTableSet(t_Handle h_FmPcd, t_FmPcdCcNode *p_CcNode,

```
....
4815.          NextStepAd(p_AdTableTmp, NULL,
```

File Name freebsd-src-3/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1235
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5158 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	5221	255
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Error FmPcdCcTreeAddCPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5221.              NULL, &nextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c
Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1236
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4773	255
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/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 freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1237
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 3094 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3239	255
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3239.          NextStepAd(p_Ad, NULL, p_CcNextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1238
Status New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	5149	255
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5149.              NULL, &nextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1239

Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	5121	255
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5121.                   NULL, &nextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
255.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1240
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	881	239
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
881.          FillAdOfTypeContLookup(h_Ad, NULL, p_CcNode->h_FmPcd,
p_FmPcdCcNodeTmp,
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      if (p_FmPcdCcStatsParams->h_StatsFLRs)
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1241
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 834 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	890	239
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method static t_Handle BuildNewAd(

```
....
890.                  h_Ad, NULL, p_CcNode->h_FmPcd, p_FmPcdCcNodeTmp,
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1242
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 377 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	403	239
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/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 freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.       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=1060099&projectid=60089&pathid=1243
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 2566 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	2686	239
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeAddOrMdfyKeyAndNextEngine(

```
....
2686.                   NextStepAd(p_AdTableNewTmp, NULL,
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1244
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4815	239
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/fm_cc.c

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

```
....
4815.          NextStepAd(p_AdTableTmp, NULL,
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1245
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	5121	239

Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5121.                   NULL, &nextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1246
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 3094 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3239	239
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error BuildNewNodeModifyNextEngine(

```
....
3239.          NextStepAd(p_Ad, NULL, p_CcNextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1247
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5046 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	5149	239
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method t_Error FmPcdCcTreeAddIPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5149.               NULL, &nextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1248
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5994 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	6197	239
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method t_Handle FM_PCD_CcRootBuild(t_Handle h_FmPcd,

```
....
6197.          NextStepAd(p_CcTreeTmp, NULL,
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1249
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 5158 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	5221	239
Object	null	h_StatsFLRs

Code Snippet

File Name freebsd-src-3/fm_cc.c

Method t_Error FmPcdCcTreeAddCPR(t_Handle h_FmPcd, t_Handle h_FmTree,

```
....
5221.              NULL, &nextEngineParams, h_FmPcd);
```

File Name freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1250
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 4324 is not initialized when it is used by h_StatsFLRs at freebsd-src-3/fm_cc.c in line 225.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	4773	239
Object	null	h_StatsFLRs

Code Snippet
File Name freebsd-src-3/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 freebsd-src-3/fm_cc.c

Method static void UpdateStatsAd(t_FmPcdCcStatsParams *p_FmPcdCcStatsParams,

```
....
239.      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=1060099&projectid=60089&pathid=1251
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 3551 is not initialized when it is used by params at freebsd-src-3/fm_cc.c in line 834.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3556	892
Object	null	params

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error UpdatePtrWhichPointOnCrntMdfNode(

```
....
3556.      t_FmPcdCcNextEngineParams *p_NextEngineParams = NULL;
```

File Name freebsd-src-3/fm_cc.c

Method	static t_Handle BuildNewAd(

```
....
892.                    p_FmPcdCcNextEngineParams-
>params.frParams.h_FrmReplic);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1252
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 3551 is not initialized when it is used by params at freebsd-src-3/fm_cc.c in line 834.

	Source	Destination
File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3556	887
Object	null	params

Code Snippet

File Name	freebsd-src-3/fm_cc.c
Method	static t_Error UpdatePtrWhichPointOnCrntMdfNode(

```
....
3556.      t_FmPcdCcNextEngineParams *p_NextEngineParams = NULL;
```

File Name	freebsd-src-3/fm_cc.c
Method	static t_Handle BuildNewAd(

```
....
887.               && (p_FmPcdCcNextEngineParams-
>params.frParams.h_FrmReplic))
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1253
Status	New

The variable declared in null at freebsd-src-3/fm_cc.c in line 3551 is not initialized when it is used by params at freebsd-src-3/fm_cc.c in line 834.

	Source	Destination

File	freebsd-src-3/fm_cc.c	freebsd-src-3/fm_cc.c
Line	3556	873
Object	null	params

Code Snippet
File Name freebsd-src-3/fm_cc.c
Method static t_Error UpdatePtrWhichPointOnCrntMdfNode(

```
....
3556.      t_FmPcdCcNextEngineParams *p_NextEngineParams = NULL;
```

File Name freebsd-src-3/fm_cc.c
Method static t_Handle BuildNewAd(

```
....
873.                       p_FmPcdCcNextEngineParams-
>params.ccParams.h_CcNode)
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1254
Status	New

The variable declared in null at freebsd-src-3/htt_rx.c in line 3928 is not initialized when it is used by def at freebsd-src-3/htt_rx.c in line 3928.

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	3933	3990
Object	null	def

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method ath10k_update_per_peer_tx_stats(struct ath10k *ar,

```
....
3933.       struct ieee80211_chanctx_conf *conf = NULL;
....
3990.             if (conf && conf->def.chan->band == NL80211_BAND_5GHZ)
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=600

	89&pathid=1255
Status	New

The variable declared in null at freebsd-src-3/icmp6.c in line 2014 is not initialized when it is used by ip6_src at freebsd-src-3/icmp6.c in line 2014.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2069	2122
Object	null	ip6_src

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_reflect(struct mbuf *m, size_t off)

```
....
2069.        srcp = NULL;
....
2122.        ip6->ip6_src = *srcp;
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1256
Status	New

The variable declared in null at freebsd-src-3/irdma_cm.c in line 1852 is not initialized when it is used by cm_id at freebsd-src-3/irdma_cm.c in line 3929.

	Source	Destination
File	freebsd-src-3/irdma_cm.c	freebsd-src-3/irdma_cm.c
Line	1930	3941
Object	null	cm_id

Code Snippet
File Name freebsd-src-3/irdma_cm.c
Method irdma_dec_refcnt_listen(struct irdma_cm_core *cm_core,

```
....
1930.              listener = NULL;
```

File Name freebsd-src-3/irdma_cm.c
Method irdma_destroy_listen(struct iw_cm_id *cm_id)

```
....
3941.       cm_id->rem_ref(cm_id);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1257
Status	New

The variable declared in null at freebsd-src-3/iter_utils.c in line 1417 is not initialized when it is used by dp at freebsd-src-3/iter_utils.c in line 1417.

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1432	1451
Object	null	dp

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method iter_stub_fwd_no_cache(struct module_qstate *qstate, struct query_info *qinf,

```
....
1432.                   stub = NULL; /* ignore stub, forward is lower */
....
1451.             return (stub->dp->no_cache);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1258
Status	New

The variable declared in null at freebsd-src-3/iter_utils.c in line 1417 is not initialized when it is used by dp at freebsd-src-3/iter_utils.c in line 1417.

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1432	1449
Object	null	dp

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method iter_stub_fwd_no_cache(struct module_qstate *qstate, struct query_info *qinf,

```
....
1432.                   stub = NULL; /* ignore stub, forward is lower */
....
1449.                   *retdpnamelen = stub->dp->namelen;
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1259
Status	New

The variable declared in null at freebsd-src-3/iter_utils.c in line 1417 is not initialized when it is used by dp at freebsd-src-3/iter_utils.c in line 1417.

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1432	1448
Object	null	dp

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method iter_stub_fwd_no_cache(struct module_qstate *qstate, struct query_info *qinf,

```
....
1432.                   stub = NULL; /* ignore stub, forward is lower */
....
1448.                   *retdpname = stub->dp->name;
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1260
Status	New

The variable declared in null at freebsd-src-3/iter_utils.c in line 1417 is not initialized when it is used by dp at freebsd-src-3/iter_utils.c in line 1417.

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1432	1444
Object	null	dp

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method iter_stub_fwd_no_cache(struct module_qstate *qstate, struct query_info *qinf,

```
....
1432.                    stub = NULL; /* ignore stub, forward is lower */
....
1444.                    dname_str(stub->dp->name, dpname);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1261
Status	New

The variable declared in null at freebsd-src-3/iter_utils.c in line 1417 is not initialized when it is used by dp at freebsd-src-3/iter_utils.c in line 1417.

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1432	1440
Object	null	dp

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method iter_stub_fwd_no_cache(struct module_qstate *qstate, struct query_info *qinf,

```
....
1432.                    stub = NULL; /* ignore stub, forward is lower */
....
1440.             if(stub->dp->no_cache) {
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1262
Status	New

The variable declared in null at freebsd-src-3/mlx5_ib_cq.c in line 670 is not initialized when it is used by ibqp at freebsd-src-3/mlx5_ib_cq.c in line 166.

	Source	Destination
File	freebsd-src-3/mlx5_ib_cq.c	freebsd-src-3/mlx5_ib_cq.c
Line	673	230
Object	null	ibqp

Code Snippet
File Name freebsd-src-3/mlx5_ib_cq.c
Method int mlx5_ib_poll_cq(struct ib_cq *ibcq, int num_entries, struct ib_wc *wc)

```
....
673.        struct mlx5_ib_qp *cur_qp = NULL;
```

File Name freebsd-src-3/mlx5_ib_cq.c

Method static void handle_responder(struct ib_wc *wc, struct mlx5_cqe64 *cqe,

```
....
230.        if (unlikely(is_qp1(qp->ibqp.qp_type))) {
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1263
Status	New

The variable declared in null at freebsd-src-3/mlx5_ib_cq.c in line 670 is not initialized when it is used by ibqp at freebsd-src-3/mlx5_ib_cq.c in line 166.

	Source	Destination
File	freebsd-src-3/mlx5_ib_cq.c	freebsd-src-3/mlx5_ib_cq.c
Line	673	181
Object	null	ibqp

Code Snippet

File Name freebsd-src-3/mlx5_ib_cq.c

Method int mlx5_ib_poll_cq(struct ib_cq *ibcq, int num_entries, struct ib_wc *wc)

```
....
673.        struct mlx5_ib_qp *cur_qp = NULL;
```

File Name freebsd-src-3/mlx5_ib_cq.c

Method static void handle_responder(struct ib_wc *wc, struct mlx5_cqe64 *cqe,

```
....
181.            if (qp->ibqp.xrcd) {
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1264
Status	New

The variable declared in null at freebsd-src-3/mlx5_ib_cq.c in line 670 is not initialized when it is used by ibqp at freebsd-src-3/mlx5_ib_cq.c in line 166.

	Source	Destination
File	freebsd-src-3/mlx5_ib_cq.c	freebsd-src-3/mlx5_ib_cq.c
Line	673	178
Object	null	ibqp

Code Snippet
File Name freebsd-src-3/mlx5_ib_cq.c
Method int mlx5_ib_poll_cq(struct ib_cq *ibcq, int num_entries, struct ib_wc *wc)

```
....
673.        struct mlx5_ib_qp *cur_qp = NULL;
```

File Name freebsd-src-3/mlx5_ib_cq.c

Method static void handle_responder(struct ib_wc *wc, struct mlx5_cqe64 *cqe,

```
....
178.        if (qp->ibqp.srq || qp->ibqp.xrcd) {
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1265
Status	New

The variable declared in null at freebsd-src-3/mlx5_ib_cq.c in line 670 is not initialized when it is used by ibqp at freebsd-src-3/mlx5_ib_cq.c in line 166.

	Source	Destination
File	freebsd-src-3/mlx5_ib_cq.c	freebsd-src-3/mlx5_ib_cq.c
Line	673	178
Object	null	ibqp

Code Snippet
File Name freebsd-src-3/mlx5_ib_cq.c
Method int mlx5_ib_poll_cq(struct ib_cq *ibcq, int num_entries, struct ib_wc *wc)

```
....
673.        struct mlx5_ib_qp *cur_qp = NULL;
```

File Name freebsd-src-3/mlx5_ib_cq.c

Method	static void handle_responder(struct ib_wc *wc, struct mlx5_cqe64 *cqe,

```
....
178.        if (qp->ibqp.srq || qp->ibqp.xrcd) {
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1266
Status	New

The variable declared in null at freebsd-src-3/pk7_lib.c in line 547 is not initialized when it is used by flags at freebsd-src-3/pk7_lib.c in line 547.

	Source	Destination
File	freebsd-src-3/pk7_lib.c	freebsd-src-3/pk7_lib.c
Line	577	584
Object	null	flags

Code Snippet	
File Name	freebsd-src-3/pk7_lib.c
Method	int PKCS7_stream(unsigned char ***boundary, PKCS7 *p7)

```
....
577.           os = NULL;
....
584.       os->flags |= ASN1_STRING_FLAG_NDEF;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1267
Status	New

The variable declared in null at freebsd-src-3/pkinit.c in line 1639 is not initialized when it is used by realm at freebsd-src-3/pkinit.c in line 1639.

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1647	1695
Object	null	realm

Code Snippet	
File Name	freebsd-src-3/pkinit.c
Method	match_ms_upn_san(krb5_context context,

```
....
1647.      krb5_principal principal = NULL;
....
1695.       strupr(principal->realm);
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1268
Status	New

The variable declared in 0 at freebsd-src-3/htt_rx.c in line 784 is not initialized when it is used by Pointer at freebsd-src-3/htt_rx.c in line 784.

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	833	833
Object	0	Pointer

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method int ath10k_htt_rx_alloc(struct ath10k_htt *htt)

```
....
833.        *htt->rx_ring.alloc_idx.vaddr = 0;
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1269
Status	New

The variable declared in 0 at freebsd-src-3/if_bwn_phy_g.c in line 3316 is not initialized when it is used by padmix at freebsd-src-3/if_bwn_phy_g.c in line 3316.

	Source	Destination
File	freebsd-src-3/if_bwn_phy_g.c	freebsd-src-3/if_bwn_phy_g.c
Line	3334	3334
Object	0	padmix

Code Snippet
File Name freebsd-src-3/if_bwn_phy_g.c
Method bwn_phy_g_set_txpwr_sub(struct bwn_mac *mac, const struct bwn_bbatt *bbatt,

```
....
3334.       pg->pg_rfatt.padmix = (txctl & BWN_TXCTL_TXMIX) ? 1 : 0;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1270
Status	New

The variable declared in 0 at freebsd-src-3/mlx5_ib_cq.c in line 166 is not initialized when it is used by wc_flags at freebsd-src-3/mlx5_ib_cq.c in line 166.

	Source	Destination
File	freebsd-src-3/mlx5_ib_cq.c	freebsd-src-3/mlx5_ib_cq.c
Line	229	229
Object	0	wc_flags

Code Snippet
File Name freebsd-src-3/mlx5_ib_cq.c
Method static void handle_responder(struct ib_wc *wc, struct mlx5_cqe64 *cqe,

```
....
229.        wc->wc_flags |= g ? IB_WC_GRH : 0;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1271
Status	New

The variable declared in 0 at freebsd-src-3/mlx5_ib_cq.c in line 166 is not initialized when it is used by wc_flags at freebsd-src-3/mlx5_ib_cq.c in line 166.

	Source	Destination
File	freebsd-src-3/mlx5_ib_cq.c	freebsd-src-3/mlx5_ib_cq.c
Line	229	267
Object	0	wc_flags

Code Snippet
File Name freebsd-src-3/mlx5_ib_cq.c
Method static void handle_responder(struct ib_wc *wc, struct mlx5_cqe64 *cqe,

```
....
229.        wc->wc_flags |= g ? IB_WC_GRH : 0;
....
267.        wc->wc_flags |= IB_WC_WITH_NETWORK_HDR_TYPE;
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1272
Status	New

The variable declared in 0 at freebsd-src-3/mlx5_ib_cq.c in line 166 is not initialized when it is used by wc_flags at freebsd-src-3/mlx5_ib_cq.c in line 166.

	Source	Destination
File	freebsd-src-3/mlx5_ib_cq.c	freebsd-src-3/mlx5_ib_cq.c
Line	229	251
Object	0	wc_flags

Code Snippet
File Name freebsd-src-3/mlx5_ib_cq.c
Method static void handle_responder(struct ib_wc *wc, struct mlx5_cqe64 *cqe,

```
....
229.        wc->wc_flags |= g ? IB_WC_GRH : 0;
....
251.              wc->wc_flags |= IB_WC_WITH_VLAN;
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1273
Status	New

The variable declared in 0 at freebsd-src-3/sli4.c in line 3639 is not initialized when it is used by dual_ulp_capable at freebsd-src-3/sli4.c in line 3639.

	Source	Destination
File	freebsd-src-3/sli4.c	freebsd-src-3/sli4.c
Line	3662	3662
Object	0	dual_ulp_capable

Code Snippet
File Name freebsd-src-3/sli4.c
Method sli_query_fw_config(sli4_t *sli4)

```
....
3662.              sli4->config.dual_ulp_capable = ((fw_config-
>function_mode & SLI4_FUNCTION_MODE_DUA_MODE) == 0 ? 0 : 1);
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1274
Status	New

The variable declared in 0 at freebsd-src-3/sli4.c in line 3639 is not initialized when it is used by config at freebsd-src-3/sli4.c in line 3639.

	Source	Destination
File	freebsd-src-3/sli4.c	freebsd-src-3/sli4.c
Line	3662	3679
Object	0	config

Code Snippet
File Name freebsd-src-3/sli4.c
Method sli_query_fw_config(sli4_t *sli4)

```
....
3662.              sli4->config.dual_ulp_capable = ((fw_config-
>function_mode & SLI4_FUNCTION_MODE_DUA_MODE) == 0 ? 0 : 1);
....
3679.                    } else if (sli4->config.is_ulp_fc[0]) {
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1275
Status	New

The variable declared in 0 at freebsd-src-3/sli4.c in line 3639 is not initialized when it is used by config at freebsd-src-3/sli4.c in line 3639.

	Source	Destination
File	freebsd-src-3/sli4.c	freebsd-src-3/sli4.c
Line	3662	3675
Object	0	config

Code Snippet
File Name freebsd-src-3/sli4.c
Method sli_query_fw_config(sli4_t *sli4)

```
....
3662.              sli4->config.dual_ulp_capable = ((fw_config-
>function_mode & SLI4_FUNCTION_MODE_DUA_MODE) == 0 ? 0 : 1);
....
3675.                    if (sli4->config.is_ulp_fc[0] &&
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1276
Status	New

The variable declared in 0 at freebsd-src-3/sli4.c in line 3639 is not initialized when it is used by config at freebsd-src-3/sli4.c in line 3639.

	Source	Destination
File	freebsd-src-3/sli4.c	freebsd-src-3/sli4.c
Line	3662	3676
Object	0	config

Code Snippet
File Name freebsd-src-3/sli4.c
Method sli_query_fw_config(sli4_t *sli4)

```
....
3662.              sli4->config.dual_ulp_capable = ((fw_config-
>function_mode & SLI4_FUNCTION_MODE_DUA_MODE) == 0 ? 0 : 1);
....
3676.                         sli4->config.is_ulp_fc[1]) {
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1277
Status	New

The variable declared in 0 at freebsd-src-3/sli4.c in line 3639 is not initialized when it is used by config at freebsd-src-3/sli4.c in line 3639.

	Source	Destination
File	freebsd-src-3/sli4.c	freebsd-src-3/sli4.c
Line	3662	3670
Object	0	config

Code Snippet

File Name	freebsd-src-3/sli4.c
Method	sli_query_fw_config(sli4_t *sli4)

```
....
3662.              sli4->config.dual_ulp_capable = ((fw_config-
>function_mode & SLI4_FUNCTION_MODE_DUA_MODE) == 0 ? 0 : 1);
....
3670.              if (sli4->config.dual_ulp_capable) {
```

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=1060099&projectid=60089&pathid=1558
Status	New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1528	1528
Object	fgets	fgets

Code Snippet

File Name	freebsd-src-3/hxtool.c
Method	hxtool_hex(struct hex_options *opt, int argc, char **argv)

```
....
1528.       while(fgets(buf, sizeof(buf), stdin) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1559
Status	New

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1919	1919

Object	fgets	fgets

Code Snippet
File Name freebsd-src-3/pkinit.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1919.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1560
Status New

	Source	Destination
File	freebsd-src-3/test_tparm.c	freebsd-src-3/test_tparm.c
Line	254	254
Object	fgets	fgets

Code Snippet
File Name freebsd-src-3/test_tparm.c
Method main(int argc, char *argv[])

```
....
254.            while (fgets(buffer, sizeof(buffer) - 1, stdin) != 0) {
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1561
Status New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1528	1528
Object	buf	buf

Code Snippet
File Name freebsd-src-3/hxtool.c
Method hxtool_hex(struct hex_options *opt, int argc, char **argv)

```
....
1528.       while(fgets(buf, sizeof(buf), stdin) != NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1562
Status	New

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1919	1919
Object	buf	buf

Code Snippet
File Name freebsd-src-3/pkinit.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1919.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1563
Status	New

	Source	Destination
File	freebsd-src-3/test_tparm.c	freebsd-src-3/test_tparm.c
Line	254	254
Object	buffer	buffer

Code Snippet
File Name freebsd-src-3/test_tparm.c
Method main(int argc, char *argv[])

```
....
254.            while (fgets(buffer, sizeof(buffer) - 1, stdin) != 0) {
```

Improper Resource Access Authorization\Path 7:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1564
Status	New

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	490	490
Object	buf	buf

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
490.              while ((s = fread(buf, 1, sizeof(buf), f)) > 0) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1565
Status	New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1543	1543
Object	buf	buf

Code Snippet
File Name freebsd-src-3/hxtool.c
Method hxtool_hex(struct hex_options *opt, int argc, char **argv)

```
....
1543.       while((len = fread(buf, 1, sizeof(buf), stdin)) != 0) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1566
Status	New

	Source	Destination
File	freebsd-src-3/zuncompress.c	freebsd-src-3/zuncompress.c
Line	362	362

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name freebsd-src-3/zuncompress.c
Method getcode(struct s_zstate *zs)

```
....
362.              zs->u.r.zs_size = fread(zs->u.r.zs_gbuf + i, 1, zs-
>zs_n_bits - i, zs->zs_fp);
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1567
Status New

	Source	Destination
File	freebsd-src-3/zuncompress.c	freebsd-src-3/zuncompress.c
Line	150	150
Object	buf	buf

Code Snippet
File Name freebsd-src-3/zuncompress.c
Method zuncompress(FILE *in, FILE *out, char *pre, size_t prelen,

```
....
150.        while ((bin = fread(buf, 1, BUFSIZE, in)) != 0) {
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1568
Status New

	Source	Destination
File	freebsd-src-3/zuncompress.c	freebsd-src-3/zuncompress.c
Line	240	240
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name freebsd-src-3/zuncompress.c
Method zread(void *cookie, char *rbp, int num)

```
....
240.        if (fread(header + i, 1, sizeof(header) - i, zs->zs_fp) !=
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1569
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	248	248
Object	Address	Address

Code Snippet
File Name freebsd-src-3/chutest.c
Method process_raw(

```
....
248.        while ((n = read(s, &c, sizeof(char))) > 0) {
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1570
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	355	355
Object	Address	Address

Code Snippet
File Name freebsd-src-3/chutest.c
Method process_ldisc(

```
....
355.        while ((n = read(s, (char *)&chu, sizeof chu)) > 0) {
```

Improper Resource Access Authorization\Path 14:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1571
Status	New

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1152	1152
Object	buf	buf

Code Snippet
File Name freebsd-src-3/nfsd.c
Method copy_stable(int from_fd, int to_fd)

```
....
1152.                   cnt = read(from_fd, buf, 1024);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1572
Status	New

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1527	1527
Object	data	data

Code Snippet
File Name freebsd-src-3/pkinit.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1527.           ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1573
Status	New

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1963	1963

Object	buf	buf

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method receiver_body(void *data)

```
....
1963.             i = read(targ->g->main_fd, buf, sizeof(buf));
```

Improper Resource Access Authorization\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1574
Status New

	Source	Destination
File	freebsd-src-3/utility.c	freebsd-src-3/utility.c
Line	62	62
Object	netibuf	netibuf

Code Snippet
File Name freebsd-src-3/utility.c
Method ttloop(void)

```
....
62.      ncc = read(net, netibuf, sizeof netibuf);
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1575
Status New

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	207	207
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method usage(void)

```
....
207.        fprintf(stderr,
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1576
Status	New

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	125	125
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method do_bthid_command(bdaddr_p bdaddr, int argc, char **argv)

```
....
125.                    fprintf(stdout, "Supported commands:\n");
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1577
Status	New

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	143	143
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method do_bthid_command(bdaddr_p bdaddr, int argc, char **argv)

```
....
143.                fprintf(stdout, "Unknown command: \"%s\"\n", cmd);
```

Improper Resource Access Authorization\Path 21:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1578
Status	New

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	158	158
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method do_bthid_command(bdaddr_p bdaddr, int argc, char **argv)

```
....
158.                fprintf(stdout, "Could not execute command \"%s\".
%s\n",
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1579
Status	New

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	163	163
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method do_bthid_command(bdaddr_p bdaddr, int argc, char **argv)

```
....
163.                fprintf(stdout, "Usage: %s\n%s\n", c->command, c-
>description);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1580
Status	New

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c

Line	200	200
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method print_bthid_command(struct bthid_command *category)

```
....
200.              fprintf(stdout, "\t%s\n", c->command);
```

Improper Resource Access Authorization\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1581
Status New

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	188	188
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
188.                    fprintf(stderr, "Invalid block size %d\n",
blksize);
```

Improper Resource Access Authorization\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1582
Status New

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	214	214
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
214.                    fprintf(stderr, "Invalid implementation %s\n",
optarg);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1583
Status	New

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	225	225
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
225.                    fprintf(stderr, "Invalid number of operations
%d\n", numops);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1584
Status	New

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	236	236
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
236.                    fprintf(stderr, "Invalid pool size %d\n",
poolsize);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1585
Status	New

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	256	256
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
256.                fprintf(stderr, "Usage: checksum <options>\n"
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1586
Status	New

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	109	109
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chksum.c
Method verify(const void *data, uint32_t offset, uint32_t size)

```
....
109.        fprintf(stderr, "\nInvalid checksum for offset %u size %u: "
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1587
Status	New

	Source	Destination

File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	133	133
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method main(

```
....
133.              (void) fprintf(stderr, "usage: %s [-dft]
tty_device\n",
```

Improper Resource Access Authorization\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1588
Status New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	137	137
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method main(

```
....
137.              (void) fprintf(stderr, "usage: %s [-dft]
tty_device\n",
```

Improper Resource Access Authorization\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1589
Status New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	142	142
Object	fprintf	fprintf

Code Snippet

File Name	freebsd-src-3/chutest.c
Method	main(

```
....
142.                (void) fprintf(stderr, "usage: %s [-cdft]
tty_device\n",
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1590
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	179	179
Object	fprintf	fprintf

Code Snippet

File Name	freebsd-src-3/chutest.c
Method	openterm(

```
....
179.            (void) fprintf(stderr, "Doing open...");
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1591
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	183	183
Object	fprintf	fprintf

Code Snippet

File Name	freebsd-src-3/chutest.c
Method	openterm(

```
....
183.            (void) fprintf(stderr, "open okay\n");
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1592
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	186	186
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
186.            (void) fprintf(stderr, "Setting exclusive use...");
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1593
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	190	190
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
190.            (void) fprintf(stderr, "done\n");
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1594
Status	New

	Source	Destination

File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	196	196
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
196.            (void) fprintf(stderr, "Setting baud rate et al...");
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1595
Status New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	200	200
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
200.            (void) fprintf(stderr, "done\n");
```

Improper Resource Access Authorization\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1596
Status New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	207	207
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
207.                    (void) fprintf(stderr, "Switching to CHU
ldisc...");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1597
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	212	212
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
212.                    (void) fprintf(stderr, "okay\n");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1598
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	219	219
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
219.                    (void) fprintf(stderr, "Poping off streams...");
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1599
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	222	222
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
222.                    (void) fprintf(stderr, "okay\n");
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1600
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	224	224
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
224.                    (void) fprintf(stderr, "Pushing CHU stream...");
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1601
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c

Line	228	228
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
228.                    (void) fprintf(stderr, "okay\n");
```

Improper Resource Access Authorization\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1602
Status New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	267	267
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method process_raw(

```
....
267.                (void) fprintf(stderr, "%s: zero returned on read\n",
progname);
```

Improper Resource Access Authorization\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1603
Status New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	289	289
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method raw_filter(

```
....
289.                    (void) fprintf(stderr,
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1604
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	357	357
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method process_ldisc(

```
....
357.                    (void) fprintf(stderr, "Expected %d, got %d\n",
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1605
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	388	388
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method process_ldisc(

```
....
388.                (void) fprintf(stderr, "%s: zero returned on read\n",
progname);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1606
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	406	406
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method error(

```
....
406.        (void) fprintf(stderr, "%s: ", progname);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1607
Status	New

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	407	407
Object	fprintf	fprintf

Code Snippet
File Name freebsd-src-3/chutest.c
Method error(

```
....
407.        (void) fprintf(stderr, fmt, s1, s2);
```

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=1060099&projectid=60089&pathid=1345
Status	New

Method cpuctl_do_cpuid in freebsd-src-3/cpuctl.c, at line 238, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/cpuctl.c	freebsd-src-3/cpuctl.c
Line	247	247
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/cpuctl.c
Method cpuctl_do_cpuid(int cpu, cpuctl_cpuid_args_t *data, struct thread *td)

```
....
247.        bcopy(cdata.data, data->data, sizeof(data->data)); /* Ignore
error */
```

Use of Obsolete Functions\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1346
Status	New

Method freebsd32_cmsg_convert in freebsd-src-3/freebsd32_misc.c, at line 1351, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	1400	1400
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_cmsg_convert(const struct cmsghdr *cm, void *data, socklen_t datalen)

```
....
1400.       bcopy(&tmp32, data, copylen);
```

Use of Obsolete Functions\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1347

Status	New

Method freebsd32_kldstat in freebsd-src-3/freebsd32_misc.c, at line 3694, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	3711	3711
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_kldstat(struct thread *td, struct freebsd32_kldstat_args *uap)

```
....
3711.             bcopy(&stat->name[0], &stat32->name[0], sizeof(stat-
>name));
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1348
Status	New

Method freebsd32_kldstat in freebsd-src-3/freebsd32_misc.c, at line 3694, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/freebsd32_misc.c	freebsd-src-3/freebsd32_misc.c
Line	3716	3716
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/freebsd32_misc.c
Method freebsd32_kldstat(struct thread *td, struct freebsd32_kldstat_args *uap)

```
....
3716.             bcopy(&stat->pathname[0], &stat32->pathname[0],
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1349
Status	New

Method icmp6_input in freebsd-src-3/icmp6.c, at line 441, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	578	578
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
578.                    bcopy(ip6, nip6, sizeof(struct ip6_hdr));
```

Use of Obsolete Functions\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1350
Status	New

Method icmp6_input in freebsd-src-3/icmp6.c, at line 441, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	580	580
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
580.                    bcopy(icmp6, nicmp6, sizeof(struct icmp6_hdr));
```

Use of Obsolete Functions\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1351
Status	New

Method icmp6_input in freebsd-src-3/icmp6.c, at line 441, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	716	716

Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
716.                    bcopy(ip6, nip6, sizeof(struct ip6_hdr));
```

Use of Obsolete Functions\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1352
Status New

Method icmp6_input in freebsd-src-3/icmp6.c, at line 441, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	718	718
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
718.                    bcopy(icmp6, nicmp6, sizeof(struct icmp6_hdr));
```

Use of Obsolete Functions\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1353
Status New

Method icmp6_input in freebsd-src-3/icmp6.c, at line 441, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	729	729
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c

Method	icmp6_input(struct mbuf **mp, int *offp, int proto)

```
....
729.                    bcopy(pr->pr_hostname, p + 4, maxhlen);
```

Use of Obsolete Functions\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1354
Status	New

Method ni6_input in freebsd-src-3/icmp6.c, at line 1193, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1441	1441
Object	bcopy	bcopy

Code Snippet	
File Name	freebsd-src-3/icmp6.c
Method	ni6_input(struct mbuf *m, int off, struct prison *pr)

```
....
1441.       bcopy(mtod(m, caddr_t), mtod(n, caddr_t), sizeof(struct
ip6_hdr));
```

Use of Obsolete Functions\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1355
Status	New

Method ni6_input in freebsd-src-3/icmp6.c, at line 1193, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1443	1443
Object	bcopy	bcopy

Code Snippet	
File Name	freebsd-src-3/icmp6.c
Method	ni6_input(struct mbuf *m, int off, struct prison *pr)

```
....
1443.       bcopy((caddr_t)ni6, (caddr_t)nni6, sizeof(struct
icmp6_nodeinfo));
```

Use of Obsolete Functions\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1356
Status	New

Method ni6_input in freebsd-src-3/icmp6.c, at line 1193, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1458	1458
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_input(struct mbuf *m, int off, struct prison *pr)

```
....
1458.             bcopy(&v, nni6 + 1, sizeof(u_int32_t));
```

Use of Obsolete Functions\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1357
Status	New

Method ni6_nametodns in freebsd-src-3/icmp6.c, at line 1519, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1583	1583
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_nametodns(const char *name, int namelen, int old)

```
....
1583.                   bcopy(p, cp, i);
```

Use of Obsolete Functions\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1358
Status	New

Method ni6_store_addrs in freebsd-src-3/icmp6.c, at line 1763, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1871	1871
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1871.                   bcopy(&ltime, cp, sizeof(u_int32_t));
```

Use of Obsolete Functions\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1359
Status	New

Method ni6_store_addrs in freebsd-src-3/icmp6.c, at line 1763, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1875	1875
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method ni6_store_addrs(struct icmp6_nodeinfo *ni6, struct icmp6_nodeinfo *nni6,

```
....
1875.                   bcopy(&ifa6->ia_addr.sin6_addr, cp,
```

Use of Obsolete Functions\Path 16:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1360
Status	New

Method icmp6_rip6_input in freebsd-src-3/icmp6.c, at line 1919, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	1974	1974
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_rip6_input(struct mbuf **mp, int off)

```
....
1974.                                   bcopy(m->m_data, n->m_data, m->m_len);
```

Use of Obsolete Functions\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1361
Status	New

Method icmp6_reflect in freebsd-src-3/icmp6.c, at line 2014, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2053	2053
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_reflect(struct mbuf *m, size_t off)

```
....
2053.             bcopy((caddr_t)&nip6, mtod(m, caddr_t), sizeof(nip6));
```

Use of Obsolete Functions\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1362
Status	New

Method icmp6_redirect_input in freebsd-src-3/icmp6.c, at line 2165, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2337	2337
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_input(struct mbuf *m, int off)

```
....
2337.                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=1060099&projectid=60089&pathid=1363
Status New

Method icmp6_redirect_input in freebsd-src-3/icmp6.c, at line 2165, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2338	2338
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_input(struct mbuf *m, int off)

```
....
2338.                bcopy(&src6, &ssrc.sin6_addr, 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=1060099&projectid=60089&pathid=1364
Status New

Method icmp6_redirect_input in freebsd-src-3/icmp6.c, at line 2165, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2344	2344
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_input(struct mbuf *m, int off)

```
....
2344.                   bcopy(&redtgt6, &sgw.sin6_addr,
```

Use of Obsolete Functions\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1365
Status	New

Method icmp6_redirect_output in freebsd-src-3/icmp6.c, at line 2366, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2463	2463
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2463.       bcopy(ifp_ll6, &ip6->ip6_src, sizeof(struct in6_addr));
```

Use of Obsolete Functions\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1366
Status	New

Method icmp6_redirect_output in freebsd-src-3/icmp6.c, at line 2366, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2464	2464

Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2464.       bcopy(&sip6->ip6_src, &ip6->ip6_dst, sizeof(struct
in6_addr));
```

Use of Obsolete Functions\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1367
Status	New

Method icmp6_redirect_output in freebsd-src-3/icmp6.c, at line 2366, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2478	2478
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2478.             bcopy(router_ll6, &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=1060099&projectid=60089&pathid=1368
Status	New

Method icmp6_redirect_output in freebsd-src-3/icmp6.c, at line 2366, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2480	2480
Object	bcopy	bcopy

Code Snippet

File Name	freebsd-src-3/icmp6.c
Method	icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2480.             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=1060099&projectid=60089&pathid=1369
Status	New

Method icmp6_redirect_output in freebsd-src-3/icmp6.c, at line 2366, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2484	2484
Object	bcopy	bcopy

Code Snippet	
File Name	freebsd-src-3/icmp6.c
Method	icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2484.             bcopy(&sip6->ip6_dst, &nd_rd->nd_rd_target,
```

Use of Obsolete Functions\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1370
Status	New

Method icmp6_redirect_output in freebsd-src-3/icmp6.c, at line 2366, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2486	2486
Object	bcopy	bcopy

Code Snippet	
File Name	freebsd-src-3/icmp6.c
Method	icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2486.             bcopy(&sip6->ip6_dst, &nd_rd->nd_rd_dst,
```

Use of Obsolete Functions\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1371
Status	New

Method icmp6_redirect_output in freebsd-src-3/icmp6.c, at line 2366, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/icmp6.c	freebsd-src-3/icmp6.c
Line	2516	2516
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/icmp6.c
Method icmp6_redirect_output(struct mbuf *m0, struct nhop_object *nh)

```
....
2516.                   bcopy(ln->ll_addr, lladdr, ifp->if_addrlen);
```

Use of Obsolete Functions\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1372
Status	New

Method ti_copy_mem in freebsd-src-3/if_ti.c, at line 501, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/if_ti.c	freebsd-src-3/if_ti.c
Line	590	590
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/if_ti.c
Method ti_copy_mem(struct ti_softc *sc, uint32_t tigon_addr, uint32_t len,

```
....
590.                                bcopy(&sc->ti_membuf2[segresid],
ptr,
```

Use of Obsolete Functions\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1373
Status	New

Method ti_copy_mem in freebsd-src-3/if_ti.c, at line 501, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/if_ti.c	freebsd-src-3/if_ti.c
Line	657	657
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/if_ti.c
Method ti_copy_mem(struct ti_softc *sc, uint32_t tigon_addr, uint32_t len,

```
....
657.                            bcopy(&tmpval2, ptr, resid);
```

Use of Obsolete Functions\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1374
Status	New

Method ti_copy_mem in freebsd-src-3/if_ti.c, at line 501, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/if_ti.c	freebsd-src-3/if_ti.c
Line	675	675
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/if_ti.c
Method ti_copy_mem(struct ti_softc *sc, uint32_t tigon_addr, uint32_t len,

```
....
675.                            bcopy(ptr, &tmpval2, resid);
```

Use of Obsolete Functions\Path 31:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1375
Status	New

Method ti_copy_scratch in freebsd-src-3/if_ti.c, at line 690, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/if_ti.c	freebsd-src-3/if_ti.c
Line	763	763
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/if_ti.c
Method ti_copy_scratch(struct ti_softc *sc, uint32_t tigon_addr, uint32_t len,

```
....
763.                            bcopy(&tmpval, ptr, 4);
```

Use of Obsolete Functions\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1376
Status	New

Method ti_copy_scratch in freebsd-src-3/if_ti.c, at line 690, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/if_ti.c	freebsd-src-3/if_ti.c
Line	768	768
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/if_ti.c
Method ti_copy_scratch(struct ti_softc *sc, uint32_t tigon_addr, uint32_t len,

```
....
768.                            bcopy(ptr, &tmpval2, 4);
```

Use of Obsolete Functions\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1377
Status	New

Method ti_ioctl2 in freebsd-src-3/if_ti.c, at line 3624, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/if_ti.c	freebsd-src-3/if_ti.c
Line	3646	3646
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/if_ti.c
Method ti_ioctl2(struct cdev *dev, u_long cmd, caddr_t addr, int flag,

```
....
3646.             bcopy(&sc->ti_rdata.ti_info->ti_stats, outstats,
```

Use of Obsolete Functions\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1378
Status New

Method extract_mac_range in freebsd-src-3/pkt-gen.c, at line 492, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	503	503
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method extract_mac_range(struct mac_range *r)

```
....
503.        bcopy(e, &r->start, 6);
```

Use of Obsolete Functions\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1379
Status New

Method extract_mac_range in freebsd-src-3/pkt-gen.c, at line 492, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination

File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	504	504
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method extract_mac_range(struct mac_range *r)

```
....
504.        bcopy(e, &r->end, 6);
```

Use of Obsolete Functions\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1380
Status	New

Method initialize_packet in freebsd-src-3/pkt-gen.c, at line 1093, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1124	1124
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method initialize_packet(struct targ *targ)

```
....
1124.            bcopy(packet, (unsigned char *)targ->frame, header-
>caplen);
```

Use of Obsolete Functions\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1381
Status	New

Method initialize_packet in freebsd-src-3/pkt-gen.c, at line 1093, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1138	1138

Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method initialize_packet(struct targ *targ)

```
....
1138.             bcopy(payload, PKT(pkt, body, targ->g->af) + i, l0);
```

Use of Obsolete Functions\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1382
Status New

Method initialize_packet in freebsd-src-3/pkt-gen.c, at line 1093, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1144	1144
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method initialize_packet(struct targ *targ)

```
....
1144.       bcopy(&targ->g->src_mac.start, eh->ether_shost, 6);
```

Use of Obsolete Functions\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1383
Status New

Method initialize_packet in freebsd-src-3/pkt-gen.c, at line 1093, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1145	1145
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/pkt-gen.c

Method	initialize_packet(struct targ *targ)

```
....
1145.       bcopy(&targ->g->dst_mac.start, eh->ether_dhost, 6);
```

Use of Obsolete Functions\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1384
Status	New

Method ping_body in freebsd-src-3/pkt-gen.c, at line 1384, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1450	1450
Object	bcopy	bcopy

Code Snippet	
File Name	freebsd-src-3/pkt-gen.c
Method	ping_body(void *data)

```
....
1450.                           bcopy(&sent, p+42, sizeof(sent));
```

Use of Obsolete Functions\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1385
Status	New

Method ping_body in freebsd-src-3/pkt-gen.c, at line 1384, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1497	1497
Object	bcopy	bcopy

Code Snippet	
File Name	freebsd-src-3/pkt-gen.c
Method	ping_body(void *data)

```
....
1497.                           bcopy(p+42, &seq, sizeof(seq));
```

Use of Obsolete Functions\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1386
Status	New

Method iop_get_lct in freebsd-src-3/pst-iop.c, at line 295, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	freebsd-src-3/pst-iop.c	freebsd-src-3/pst-iop.c
Line	331	331
Object	bcopy	bcopy

Code Snippet
File Name freebsd-src-3/pst-iop.c
Method iop_get_lct(struct iop_softc *sc)

```
....
331.      bcopy(&reply->entry[0], sc->lct,
```

Reliance on DNS Lookups in a Decision

Query Path:
CPP\Cx\CPP Low Visibility\Reliance on DNS Lookups in a Decision Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-23 Session Authenticity (P1)

Description

Reliance on DNS Lookups in a Decision\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1194
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, dotp, in freebsd-src-3/addrtoname.c line 276, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	317
Object	gethostbyaddr	dotp

Code Snippet

File Name	freebsd-src-3/addrtoname.c
Method	win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.              return gethostbyaddr(addr, len, type);
```

File Name	freebsd-src-3/addrtoname.c
Method	ipaddr_string(netdissect_options *ndo, const u_char *ap)

```
....
317.                          if (dotp)
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1195
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, name, in freebsd-src-3/addrtoname.c line 276, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	311
Object	gethostbyaddr	name

Code Snippet

File Name	freebsd-src-3/addrtoname.c
Method	win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.              return gethostbyaddr(addr, len, type);
```

File Name	freebsd-src-3/addrtoname.c
Method	ipaddr_string(netdissect_options *ndo, const u_char *ap)

```
....
311.                    if (p->name == NULL)
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=600

	89&pathid=1196
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, ==, in freebsd-src-3/addrtoname.c line 276, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	311
Object	gethostbyaddr	==

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.              return gethostbyaddr(addr, len, type);
```

File Name freebsd-src-3/addrtoname.c
Method ipaddr_string(netdissect_options *ndo, const u_char *ap)

```
....
311.                    if (p->name == NULL)
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1197
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, hp, in freebsd-src-3/addrtoname.c line 276, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	307
Object	gethostbyaddr	hp

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.              return gethostbyaddr(addr, len, type);
```

File Name freebsd-src-3/addrtoname.c

Method ipaddr_string(netdissect_options *ndo, const u_char *ap)

```
....
307.              if (hp) {
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1198
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, dotp, in freebsd-src-3/addrtoname.c line 335, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	380
Object	gethostbyaddr	dotp

Code Snippet

File Name freebsd-src-3/addrtoname.c

Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.              return gethostbyaddr(addr, len, type);
```

File Name freebsd-src-3/addrtoname.c

Method ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
380.                          if (dotp)
```

Reliance on DNS Lookups in a Decision\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1199
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, name, in freebsd-src-3/addrtoname.c line 335, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	374
Object	gethostbyaddr	name

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.              return gethostbyaddr(addr, len, type);
```

File Name freebsd-src-3/addrtoname.c

Method ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
374.                      if (p->name == NULL)
```

Reliance on DNS Lookups in a Decision\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1200
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, ==, in freebsd-src-3/addrtoname.c line 335, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	374
Object	gethostbyaddr	==

Code Snippet
File Name freebsd-src-3/addrtoname.c
Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.              return gethostbyaddr(addr, len, type);
```

File Name freebsd-src-3/addrtoname.c

Method ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
374.                    if (p->name == NULL)
```

Reliance on DNS Lookups in a Decision\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1201
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 146 of freebsd-src-3/addrtoname.c. The application then makes a security decision, hp, in freebsd-src-3/addrtoname.c line 335, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/addrtoname.c	freebsd-src-3/addrtoname.c
Line	156	370
Object	gethostbyaddr	hp

Code Snippet

File Name freebsd-src-3/addrtoname.c

Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
156.                return gethostbyaddr(addr, len, type);
```

File Name freebsd-src-3/addrtoname.c

Method ip6addr_string(netdissect_options *ndo, const u_char *ap)

```
....
370.                if (hp) {
```

Reliance on DNS Lookups in a Decision\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1202
Status	New

The resolver_set_nameserver_hostname method performs a reverse DNS lookup with getaddrinfo, at line 984 of freebsd-src-3/ldns-host.c. The application then makes a security decision, err, in freebsd-src-3/ldns-host.c line 984, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	997	999
Object	getaddrinfo	err

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method resolver_set_nameserver_hostname(ldns_resolver *res, const char *server) {

```
....
997.      do err = getaddrinfo(server, NULL, &hints, &ailist);
....
999.      if (err != 0)
```

Reliance on DNS Lookups in a Decision\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1203
Status New

The resolver_set_nameserver_hostname method performs a reverse DNS lookup with getaddrinfo, at line 984 of freebsd-src-3/ldns-host.c. The application then makes a security decision, !=, in freebsd-src-3/ldns-host.c line 984, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	997	999
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method resolver_set_nameserver_hostname(ldns_resolver *res, const char *server) {

```
....
997.      do err = getaddrinfo(server, NULL, &hints, &ailist);
....
999.      if (err != 0)
```

Reliance on DNS Lookups in a Decision\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1204
Status New

The resolver_set_nameserver_hostname method performs a reverse DNS lookup with getaddrinfo, at line 984 of freebsd-src-3/ldns-host.c. The application then makes a security decision, err, in freebsd-src-3/ldns-host.c line 984, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	997	998
Object	getaddrinfo	err

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method resolver_set_nameserver_hostname(ldns_resolver *res, const char *server) {

```
....
997.      do err = getaddrinfo(server, NULL, &hints, &ailist);
998.      while (err == EAI_AGAIN);
```

Reliance on DNS Lookups in a Decision\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1205
Status New

The resolver_set_nameserver_hostname method performs a reverse DNS lookup with getaddrinfo, at line 984 of freebsd-src-3/ldns-host.c. The application then makes a security decision, ==, in freebsd-src-3/ldns-host.c line 984, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	997	998
Object	getaddrinfo	==

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method resolver_set_nameserver_hostname(ldns_resolver *res, const char *server) {

```
....
997.      do err = getaddrinfo(server, NULL, &hints, &ailist);
998.      while (err == EAI_AGAIN);
```

Reliance on DNS Lookups in a Decision\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1206
Status New

The parse_dsserver method performs a reverse DNS lookup with getaddrinfo, at line 1179 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 1179, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1283	1284
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1283.             ecode = getaddrinfo(cp, NULL, &hints, &ai_tcp);
1284.             if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1207
Status New

The parse_dsserver method performs a reverse DNS lookup with getaddrinfo, at line 1179 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 1179, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1283	1284
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method parse_dsserver(const char *optionarg, struct nfsd_nfsd_args *nfsdargp)

```
....
1283.             ecode = getaddrinfo(cp, NULL, &hints, &ai_tcp);
1284.             if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1208

Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	336	337
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
336.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp);
337.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1209
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	336	337
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
336.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp);
337.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 17:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1210
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	360	361
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
360.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp6);
361.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1211
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	360	361
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
360.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp6);
361.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1212
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	384	385
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
384.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_tcp);
385.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1213
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	384	385
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
384.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_tcp);
385.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1214
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	408	409
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
408.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_tcp6);
409.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1215
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	408	409
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
408.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_tcp6);
409.                    if (ecode != 0)
```

Reliance on DNS Lookups in a Decision\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1216
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	556	557
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
556.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp);
557.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1217
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	556	557
Object	getaddrinfo	!=

Code Snippet

File Name	freebsd-src-3/nfsd.c
Method	main(int argc, char **argv)

```
....
556.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp);
557.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1218
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	630	631
Object	getaddrinfo	ecode

Code Snippet	
File Name	freebsd-src-3/nfsd.c
Method	main(int argc, char **argv)

```
....
630.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp6);
631.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1219
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	630	631
Object	getaddrinfo	!=

Code Snippet	
File Name	freebsd-src-3/nfsd.c
Method	main(int argc, char **argv)

```
....
630.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_udp6);
631.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1220
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	701	703
Object	getaddrinfo	ecode

Code Snippet	
File Name	freebsd-src-3/nfsd.c
Method	main(int argc, char **argv)

```
....
701.                    ecode = getaddrinfo(NULL, "nfs", &hints,
....
703.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1221
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c

Line	701	703
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
701.                    ecode = getaddrinfo(NULL, "nfs", &hints,
....
703.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1222
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	780	781
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
780.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_tcp6);
781.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1223
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 158 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 158, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	780	781
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
780.                    ecode = getaddrinfo(NULL, "nfs", &hints,
&ai_tcp6);
781.                    if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1224
Status	New

The setbindhost method performs a reverse DNS lookup with getaddrinfo, at line 867 of freebsd-src-3/nfsd.c. The application then makes a security decision, ecode, in freebsd-src-3/nfsd.c line 867, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	903	904
Object	getaddrinfo	ecode

Code Snippet
File Name freebsd-src-3/nfsd.c
Method setbindhost(struct addrinfo **ai, const char *bindhost, struct addrinfo hints)

```
....
903.        ecode = getaddrinfo(hostptr, "nfs", &hints, ai);
904.        if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1225
Status	New

The setbindhost method performs a reverse DNS lookup with getaddrinfo, at line 867 of freebsd-src-3/nfsd.c. The application then makes a security decision, !=, in freebsd-src-3/nfsd.c line 867, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	903	904
Object	getaddrinfo	!=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method setbindhost(struct addrinfo **ai, const char *bindhost, struct addrinfo hints)

```
....
903.        ecode = getaddrinfo(hostptr, "nfs", &hints, ai);
904.        if (ecode != 0) {
```

Reliance on DNS Lookups in a Decision\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1226
Status New

The start_server method performs a reverse DNS lookup with getaddrinfo, at line 1019 of freebsd-src-3/nfsd.c. The application then makes a security decision, error, in freebsd-src-3/nfsd.c line 1019, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1037	1038
Object	getaddrinfo	error

Code Snippet
File Name freebsd-src-3/nfsd.c
Method start_server(int master, struct nfsd_nfsd_args *nfsdargp, const char *vhost)

```
....
1037.            error = getaddrinfo(hostname, NULL, &hints, &aip);
1038.            if (error == 0) {
```

Reliance on DNS Lookups in a Decision\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1227
Status New

The start_server method performs a reverse DNS lookup with getaddrinfo, at line 1019 of freebsd-src-3/nfsd.c. The application then makes a security decision, ==, in freebsd-src-3/nfsd.c line 1019, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1037	1038
Object	getaddrinfo	==

Code Snippet
File Name freebsd-src-3/nfsd.c
Method start_server(int master, struct nfsd_nfsd_args *nfsdargp, const char *vhost)

```
....
1037.             error = getaddrinfo(hostname, NULL, &hints, &aip);
1038.             if (error == 0) {
```

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=1060099&projectid=60089&pathid=1173
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1515	1515
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1174
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1539	1539
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1175
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1546	1546
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1176
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1551	1551
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1177
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1563	1563
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1178
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1589	1589
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1179
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1617	1617
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1180
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1637	1637
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1181
Status	New

The buffer allocated by <= in freebsd-src-3/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	freebsd-src-3/ar9300_paprd.c	freebsd-src-3/ar9300_paprd.c
Line	1709	1709
Object	<=	<=

Code Snippet
File Name freebsd-src-3/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=1060099&projectid=60089&pathid=1182
Status	New

The buffer allocated by <= in freebsd-src-3/chksum.c at line 168 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	328	328
Object	<=	<=

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
328.       for (int size = 0; size <= 256; size++)
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1183
Status	New

The buffer allocated by <= in freebsd-src-3/compile.c at line 768 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	812	812
Object	<=	<=

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_tr(char *p, struct s_tr **py)

```
....
812.              for (i = 0; i <= UCHAR_MAX; i++)
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1184
Status	New

The buffer allocated by <= in freebsd-src-3/compile.c at line 768 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	826	826
Object	<=	<=

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_tr(char *p, struct s_tr **py)

```
....
826.              for (i = 0; i <= UCHAR_MAX; i++)
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1185
Status	New

The buffer allocated by <= in freebsd-src-3/e_aes_cbc_hmac_sha1.c at line 154 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha1.c	freebsd-src-3/e_aes_cbc_hmac_sha1.c
Line	375	375
Object	<=	<=

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
375.          for (j = 0; j <= pad; j++)
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1186
Status	New

The buffer allocated by <= in freebsd-src-3/e_aes_cbc_hmac_sha256.c at line 150 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/e_aes_cbc_hmac_sha256.c	freebsd-src-3/e_aes_cbc_hmac_sha256.c
Line	390	390
Object	<=	<=

Code Snippet
File Name freebsd-src-3/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
390.          for (j = 0; j <= pad; j++)
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1187
Status	New

The buffer allocated by <= in freebsd-src-3/if_mwl.c at line 4797 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/if_mwl.c	freebsd-src-3/if_mwl.c
Line	4811	4811
Object	<=	<=

Code Snippet
File Name freebsd-src-3/if_mwl.c
Method mwl_announce(struct mwl_softc *sc)

```
....
4811.              for (i = 0; i <= WME_AC_VO; i++) {
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1188
Status	New

The buffer allocated by <= in freebsd-src-3/nfsd.c at line 158 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	840	840
Object	<=	<=

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
840.              for (tcpsock = 0; tcpsock <= maxsock; tcpsock++) {
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1189
Status	New

The buffer allocated by <= in freebsd-src-3/obj_dat.c at line 174 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/obj_dat.c	freebsd-src-3/obj_dat.c
Line	197	197
Object	<=	<=

Code Snippet
File Name freebsd-src-3/obj_dat.c
Method int OBJ_add_object(const ASN1_OBJECT *obj)

```
....
197.      for (i = ADDED_DATA; i <= ADDED_NID; i++) {
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1190
Status	New

The buffer allocated by <= in freebsd-src-3/obj_dat.c at line 174 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/obj_dat.c	freebsd-src-3/obj_dat.c
Line	214	214
Object	<=	<=

Code Snippet
File Name freebsd-src-3/obj_dat.c
Method int OBJ_add_object(const ASN1_OBJECT *obj)

```
....
214.      for (i = ADDED_DATA; i <= ADDED_NID; i++)
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1191
Status	New

The buffer allocated by <= in freebsd-src-3/print-lldp.c at line 1173 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/print-lldp.c	freebsd-src-3/print-lldp.c
Line	1259	1259
Object	<=	<=

Code Snippet
File Name freebsd-src-3/print-lldp.c
Method lldp_private_dcbx_print(netdissect_options *ndo,

```
....
1259.           for (i = 0; i <= 7; i++) {
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1192
Status	New

The buffer allocated by <= in freebsd-src-3/print-lldp.c at line 1173 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/print-lldp.c	freebsd-src-3/print-lldp.c
Line	1264	1264
Object	<=	<=

Code Snippet
File Name freebsd-src-3/print-lldp.c
Method lldp_private_dcbx_print(netdissect_options *ndo,

```
....
1264.           for (i = 0; i <= 7; i++)
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1193
Status	New

The buffer allocated by <= in freebsd-src-3/print-lldp.c at line 1173 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freebsd-src-3/print-lldp.c	freebsd-src-3/print-lldp.c
Line	1286	1286
Object	<=	<=

Code Snippet
File Name freebsd-src-3/print-lldp.c
Method lldp_private_dcbx_print(netdissect_options *ndo,

```
....
1286.           for (i = 0; i <= 7; i++)
```

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=1060099&projectid=60089&pathid=1388
Status	New

	Source	Destination
File	freebsd-src-3/wg.c	freebsd-src-3/wg.c
Line	58	58
Object	subcommands	sizeof

Code Snippet
File Name freebsd-src-3/wg.c
Method int main(int argc, const char *argv[])

```
....
58.   for (size_t i = 0; i < sizeof(subcommands) /
sizeof(subcommands[0]); ++i) {
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1389
Status	New

	Source	Destination
File	freebsd-src-3/wg.c	freebsd-src-3/wg.c
Line	58	58
Object	subcommands	sizeof

Code Snippet
File Name freebsd-src-3/wg.c
Method int main(int argc, const char *argv[])

```
....
58.   for (size_t i = 0; i < sizeof(subcommands) /
sizeof(subcommands[0]); ++i) {
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1390
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	702	702
Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
702.        if (os_snprintf_error(sizeof(buf), res))
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1391
Status	New

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	340	340
Object	uri	sizeof

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
340.        uri[sizeof(uri) - 1] = '\0';
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1392
Status	New

	Source	Destination
File	freebsd-src-3/sha1-internal.c	freebsd-src-3/sha1-internal.c
Line	303	303
Object	finalcount	sizeof

Code Snippet
File Name freebsd-src-3/sha1-internal.c
Method void SHA1Final(unsigned char digest[20], SHA1_CTX* context)

```
....
303.        forced_memzero(finalcount, sizeof(finalcount));
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1393
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	701	701
Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
701.        res = os_snprintf(buf, sizeof(buf), "BSS_TM_REQ %s",
argv[0]);
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1394
Status	New

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c

Line	45	45
Object	Pointer	sizeof

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method void SSL3_RECORD_clear(SSL3_RECORD *r, size_t num_recs)

```
....
45.          memset(&r[i], 0, sizeof(*r));
```

Sizeof Pointer Argument\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1395
Status New

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c
Line	45	45
Object	Pointer	sizeof

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method void SSL3_RECORD_clear(SSL3_RECORD *r, size_t num_recs)

```
....
45.          memset(&r[i], 0, sizeof(*r));
```

Sizeof Pointer Argument\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1396
Status New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	709	709
Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
709.              if (os_snprintf_error(sizeof(buf) - total, res))
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1397
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	708	709
Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
708.              res = os_snprintf(tmp, sizeof(buf) - total, " %s",
argv[i]);
709.              if (os_snprintf_error(sizeof(buf) - total, res))
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1398
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	702	709
Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
702.        if (os_snprintf_error(sizeof(buf), res))
....
709.              if (os_snprintf_error(sizeof(buf) - total, res))
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1399
Status	New

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	336	336
Object	uri	sizeof

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
336.              snprintf(uri, sizeof(uri) - 1, "%s", path);
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1400
Status	New

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	338	338
Object	uri	sizeof

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
338.              snprintf(uri, sizeof(uri) - 1, "%s?%s", path, query);
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1401
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	708	708
Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
708.                res = os_snprintf(tmp, sizeof(buf) - total, " %s",
argv[i]);
```

Sizeof Pointer Argument\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1402
Status New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	709	708
Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
709.                if (os_snprintf_error(sizeof(buf) - total, res))
....
708.                res = os_snprintf(tmp, sizeof(buf) - total, " %s",
argv[i]);
```

Sizeof Pointer Argument\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1403
Status New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	702	708

Object	buf	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static int hostapd_cli_cmd_bss_tm_req(struct wpa_ctrl *ctrl, int argc,

```
....
702.        if (os_snprintf_error(sizeof(buf), res))
....
708.                res = os_snprintf(tmp, sizeof(buf) - total, " %s",
argv[i]);
```

Sizeof Pointer Argument\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1404
Status New

	Source	Destination
File	freebsd-src-3/ssl3_record.c	freebsd-src-3/ssl3_record.c
Line	1423	1423
Object	header	sizeof

Code Snippet
File Name freebsd-src-3/ssl3_record.c
Method int tls1_mac(SSL *ssl, SSL3_RECORD *rec, unsigned char *md, int sending)

```
....
1423.          if (EVP_DigestSignUpdate(mac_ctx, header, sizeof(header))
<= 0
```

Sizeof Pointer Argument\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1405
Status New

	Source	Destination
File	freebsd-src-3/utility.c	freebsd-src-3/utility.c
Line	776	776
Object	tbuf	sizeof

Code Snippet
File Name freebsd-src-3/utility.c
Method printsub(int direction, unsigned char *pointer, size_t length)

```
....
776.                    sizeof(tbuf),
```

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=1060099&projectid=60089&pathid=1683
Status	New

The main method in freebsd-src-3/https-client.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	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	479	479
Object	fopen	fopen

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
479.              FILE * f = fopen(data_file, "rb");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1684
Status	New

The cms_verify_sd method in freebsd-src-3/hxtool.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	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name freebsd-src-3/hxtool.c

Method	cms_verify_sd(struct cms_verify_sd_options *opt, int argc, char **argv)

```
....
220.        f = fopen(argv[0], "r");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1685
Status	New

The cms_create_sd method in freebsd-src-3/hxtool.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	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	486	486
Object	fopen	fopen

Code Snippet	
File Name	freebsd-src-3/hxtool.c
Method	cms_create_sd(struct cms_create_sd_options *opt, int argc, char **argv)

```
....
486.        f = fopen(outfile, "w");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1686
Status	New

The ocsp_fetch method in freebsd-src-3/hxtool.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	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1107	1107
Object	fopen	fopen

Code Snippet	
File Name	freebsd-src-3/hxtool.c
Method	ocsp_fetch(struct ocsp_fetch_options *opt, int argc, char **argv)

```
....
1107.       f = fopen(file, "w");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1687
Status	New

The load_mappings method in freebsd-src-3/pkinit.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	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1915	1915
Object	fopen	fopen

Code Snippet
File Name freebsd-src-3/pkinit.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1915.       f = fopen(fn, "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1688
Status	New

The att_test method in freebsd-src-3/t_regex_att.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	freebsd-src-3/t_regex_att.c	freebsd-src-3/t_regex_att.c
Line	394	394
Object	fopen	fopen

Code Snippet
File Name freebsd-src-3/t_regex_att.c
Method att_test(const struct atf_tc *tc, const char *data_name)

```
....
394.        input_file = fopen(data_path, "r");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1689
Status	New

The openterm method in freebsd-src-3/chutest.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	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	180	180
Object	open	open

Code Snippet
File Name freebsd-src-3/chutest.c
Method openterm(

```
....
180.        if ((s = open(dev, O_RDONLY, 0777)) < 0)
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1690
Status	New

The compile_stream method in freebsd-src-3/compile.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	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	289	289
Object	open	open

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_stream(struct s_command **link)

```
....
289.                    else if ((cmd->u.fd = open(p,
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1691
Status	New

The compile_flags method in freebsd-src-3/compile.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	freebsd-src-3/compile.c	freebsd-src-3/compile.c
Line	750	750
Object	open	open

Code Snippet
File Name freebsd-src-3/compile.c
Method compile_flags(char *p, struct s_subst *s)

```
....
750.                    if (!aflag && (s->wfd = open(wfile,
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1692
Status	New

The open_stable method in freebsd-src-3/nfsd.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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1094	1094
Object	open	open

Code Snippet
File Name freebsd-src-3/nfsd.c
Method open_stable(int *stable_fdp, int *backup_fdp)

```
....
1094.       stable_fd = open(NFSD_STABLERESTART, O_RDWR, 0);
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1693
Status	New

The open_stable method in freebsd-src-3/nfsd.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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1096	1096
Object	open	open

Code Snippet
File Name freebsd-src-3/nfsd.c
Method open_stable(int *stable_fdp, int *backup_fdp)

```
....
1096.             stable_fd = open(NFSD_STABLERESTART, O_RDWR | O_CREAT,
0600);
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1694
Status	New

The open_stable method in freebsd-src-3/nfsd.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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1107	1107
Object	open	open

Code Snippet
File Name freebsd-src-3/nfsd.c
Method open_stable(int *stable_fdp, int *backup_fdp)

```
....
1107.              backup_fd = open(NFSD_STABLEBACKUP, O_RDWR, 0);
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1695
Status	New

The open_stable method in freebsd-src-3/nfsd.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	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	1109	1109
Object	open	open

Code Snippet
File Name freebsd-src-3/nfsd.c
Method open_stable(int *stable_fdp, int *backup_fdp)

```
....
1109.                   backup_fd = open(NFSD_STABLEBACKUP, O_RDWR |
O_CREAT,
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1696
Status	New

The _kdc_pk_mk_pa_reply method in freebsd-src-3/pkinit.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	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1504	1504
Object	open	open

Code Snippet
File Name freebsd-src-3/pkinit.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1504.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1697
Status	New

The tap_alloc method in freebsd-src-3/pkt-gen.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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	2884	2884
Object	open	open

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method tap_alloc(char *dev)

```
....
2884.       if( (fd = open(clonedev, O_RDWR)) < 0 ) {
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1698
Status	New

The sparse method in freebsd-src-3/sparse.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	freebsd-src-3/sparse.c	freebsd-src-3/sparse.c
Line	28	28
Object	open	open

Code Snippet
File Name freebsd-src-3/sparse.c
Method sparse(const char *filename)

```
....
28.   if ((fd = open(filename, O_RDONLY)) < 0 ||
```

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=1060099&projectid=60089&pathid=1019
Status	New

Method update_ip at line 830 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	846	846
Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method update_ip(struct pkt *pkt, struct targ *t)

```
....
846.                    ip.ip_src.s_addr = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1020
Status	New

Method update_ip at line 830 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c

Line	847	847
Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method update_ip(struct pkt *pkt, struct targ *t)

```
....
847.                    udp.uh_sport = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1021
Status	New

Method update_ip at line 830 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	875	875
Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method update_ip(struct pkt *pkt, struct targ *t)

```
....
875.                    ip.ip_dst.s_addr = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1022
Status	New

Method update_ip at line 830 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	876	876

Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method update_ip(struct pkt *pkt, struct targ *t)

```
....
876.                    udp.uh_dport = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1023
Status	New

Method update_ip6 at line 916 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	934	934
Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method update_ip6(struct pkt *pkt, struct targ *t)

```
....
934.                    ip6.ip6_src.s6_addr16[group] = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1024
Status	New

Method update_ip6 at line 916 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	935	935
Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method update_ip6(struct pkt *pkt, struct targ *t)

```
....
935.                    udp.uh_sport = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1025
Status New

Method update_ip6 at line 916 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	966	966
Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method update_ip6(struct pkt *pkt, struct targ *t)

```
....
966.                    ip6.ip6_dst.s6_addr16[group] = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1026
Status New

Method update_ip6 at line 916 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	967	967
Object	nrand48	nrand48

Code Snippet
File Name freebsd-src-3/pkt-gen.c

Method	update_ip6(struct pkt *pkt, struct targ *t)

```
....
967.                    udp.uh_dport = nrand48(t->seed);
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1027
Status	New

Method sender_body at line 1677 of freebsd-src-3/pkt-gen.c uses a weak method nrand48 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	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	1824	1824
Object	nrand48	nrand48

Code Snippet	
File Name	freebsd-src-3/pkt-gen.c
Method	sender_body(void *data)

```
....
1824.                        size = nrand48(targ->seed) %
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1028
Status	New

Method main at line 168 of freebsd-src-3/chksum.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	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	288	288
Object	rand	rand

Code Snippet	
File Name	freebsd-src-3/chksum.c
Method	int main(int argc, char *argv[])

```
....
288.        ((uint32_t *) base)[i] = rand();
```

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=1060099&projectid=60089&pathid=1163
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	1070	1070
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static char ** hostapd_complete_set(const char *str, int pos)

```
....
1070.            res = os_calloc(num_fields + 1, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1164
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	1115	1115
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static char ** hostapd_complete_get(const char *str, int pos)

```
....
1115.            res = os_calloc(num_fields + 1, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1165
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	1927	1927
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static char ** list_cmd_list(void)

```
....
1927.       res = os_calloc(count + 1, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1166
Status	New

	Source	Destination
File	freebsd-src-3/htt_rx.c	freebsd-src-3/htt_rx.c
Line	810	810
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/htt_rx.c
Method int ath10k_htt_rx_alloc(struct ath10k_htt *htt)

```
....
810.             kcalloc(htt->rx_ring.size, sizeof(struct sk_buff *),
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1167
Status	New

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1163	1163
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method void iter_store_parentside_neg(struct module_env* env,

```
....
1163.             sizeof(uint8_t*) + sizeof(time_t) + sizeof(uint16_t));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1168
Status New

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1283	1283
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/iter_utils.c
Method iter_scrub_ds(struct dns_msg* msg, struct ub_packed_rrset_key* ns, uint8_t* z)

```
....
1283.                         sizeof(struct ub_packed_rrset_key*) *
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1169
Status New

	Source	Destination
File	freebsd-src-3/iter_utils.c	freebsd-src-3/iter_utils.c
Line	1301	1301
Object	sizeof	sizeof

Code Snippet

File Name	freebsd-src-3/iter_utils.c
Method	iter_scrub_nxdomain(struct dns_msg* msg)

```
....
1301.             sizeof(struct ub_packed_rrset_key*) *
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1170
Status	New

	Source	Destination
File	freebsd-src-3/lobject.c	freebsd-src-3/lobject.c
Line	202	202
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/lobject.c
Method const char *luaO_pushvfstring (lua_State *L, const char *fmt, va_list argp) {

```
....
202.          char buff[4*sizeof(void *) + 8]; /* should be enough space
for a `%p' */
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1171
Status	New

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	302	302
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
302.             bindhost = realloc(bindhost,sizeof(char *)*bindhostc);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1172
Status	New

	Source	Destination
File	freebsd-src-3/qlnxr_os.c	freebsd-src-3/qlnxr_os.c
Line	514	514
Object	sizeof	sizeof

Code Snippet
File Name freebsd-src-3/qlnxr_os.c
Method qlnxr_alloc_resources(struct qlnxr_dev *dev)

```
....
514.                                    sizeof(struct regpair *),
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1011
Status	New

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	70	70
Object	getopt	getopt

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method main(int argc, char *argv[])

```
....
70.   while ((opt = getopt(argc, argv, "a:c:H:hv")) != -1) {
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1012

Status	New

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	179	179
Object	getopt	getopt

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
179.      while ((c = getopt(argc, argv, "b:df:i:n:p:")) != -1)
```

Inconsistent Implementations\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1013
Status	New

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	2077	2077
Object	getopt	getopt

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method int main(int argc, char *argv[])

```
....
2077.             c = getopt(argc, argv, "a:BhG:i:p:P:rs:v");
```

Inconsistent Implementations\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1014
Status	New

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	626	626
Object	getopt	getopt

Code Snippet	
File Name	freebsd-src-3/ldns-host.c
Method	parse_args(int argc, char *argv[]) {

```
....
626.       while ((ch = getopt(argc, argv, "aCdilrsTvw46c:N:R:t:W:")) !=
-1) {
```

Inconsistent Implementations\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1015
Status	New

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	2969	2969
Object	getopt	getopt

Code Snippet	
File Name	freebsd-src-3/pkt-gen.c
Method	main(int arc, char **argv)

```
....
2969.       while ((ch = getopt(arc, argv,
"46a:f:F:Nn:i:Il:d:s:D:S:b:c:o:p:"
```

Inconsistent Implementations\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1016
Status	New

	Source	Destination
File	freebsd-src-3/sparse.c	freebsd-src-3/sparse.c
Line	54	54
Object	getopt	getopt

Code Snippet	
File Name	freebsd-src-3/sparse.c
Method	main(int argc, char *argv[])

```
....
54.    while ((opt = getopt(argc, argv, "v")) != -1) {
```

Inconsistent Implementations\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1017
Status	New

	Source	Destination
File	freebsd-src-3/test_tparm.c	freebsd-src-3/test_tparm.c
Line	190	190
Object	getopt	getopt

Code Snippet
File Name freebsd-src-3/test_tparm.c
Method main(int argc, char *argv[])

```
....
190.       while ((n = getopt(argc, argv, "T:ar:v")) != -1) {
```

Inconsistent Implementations\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1018
Status	New

	Source	Destination
File	freebsd-src-3/nfsd.c	freebsd-src-3/nfsd.c
Line	195	195
Object	getopt_long	getopt_long

Code Snippet
File Name freebsd-src-3/nfsd.c
Method main(int argc, char **argv)

```
....
195.         while ((ch = getopt_long(argc, argv, getopt_shortopts,
longopts,
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1676
Status	New

The system data read by main in the file freebsd-src-3/chksum.c at line 168 is potentially exposed by main found in freebsd-src-3/chksum.c at line 168.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	284	284
Object	perror	perror

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
284.        perror("aligned_alloc"), exit(EXIT_FAILURE);
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1677
Status	New

The system data read by main in the file freebsd-src-3/chksum.c at line 168 is potentially exposed by main found in freebsd-src-3/chksum.c at line 168.

	Source	Destination
File	freebsd-src-3/chksum.c	freebsd-src-3/chksum.c
Line	377	377
Object	perror	perror

Code Snippet
File Name freebsd-src-3/chksum.c
Method int main(int argc, char *argv[])

```
....
377.        perror("munmap"), exit(EXIT_FAILURE);
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1678
Status	New

The system data read by error in the file freebsd-src-3/chutest.c at line 400 is potentially exposed by error found in freebsd-src-3/chutest.c at line 400.

	Source	Destination
File	freebsd-src-3/chutest.c	freebsd-src-3/chutest.c
Line	409	409
Object	perror	perror

Code Snippet
File Name freebsd-src-3/chutest.c
Method error(

```
....
409.        perror("");
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1679
Status	New

The system data read by main in the file freebsd-src-3/hostapd_cli.c at line 2066 is potentially exposed by main found in freebsd-src-3/hostapd_cli.c at line 2066.

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	2152	2152
Object	perror	perror

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method int main(int argc, char *argv[])

```
....
2152.                   perror("Failed to connect to hostapd - "
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1680
Status	New

The system data read by hostapd_cli_action in the file freebsd-src-3/hostapd_cli.c at line 2029 is potentially exposed by hostapd_cli_action found in freebsd-src-3/hostapd_cli.c at line 2029.

	Source	Destination
File	freebsd-src-3/hostapd_cli.c	freebsd-src-3/hostapd_cli.c
Line	2046	2046
Object	perror	perror

Code Snippet
File Name freebsd-src-3/hostapd_cli.c
Method static void hostapd_cli_action(struct wpa_ctrl *ctrl)

```
....
2046.                   perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1681
Status	New

The system data read by main in the file freebsd-src-3/https-client.c at line 215 is potentially exposed by main found in freebsd-src-3/https-client.c at line 215.

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	416	416
Object	perror	perror

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
416.                perror("event_base_new()");
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1682
Status	New

The system data read by do_bthid_command in the file freebsd-src-3/bthidcontrol.c at line 113 is potentially exposed by do_bthid_command found in freebsd-src-3/bthidcontrol.c at line 113.

	Source	Destination
File	freebsd-src-3/bthidcontrol.c	freebsd-src-3/bthidcontrol.c
Line	159	158
Object	errno	fprintf

Code Snippet
File Name freebsd-src-3/bthidcontrol.c
Method do_bthid_command(bdaddr_p bdaddr, int argc, char **argv)

```
....
159.                            cmd, strerror(errno));
....
158.                fprintf(stdout, "Could not execute command \"%s\".
%s\n",
```

Information Exposure Through Comments

Query Path:
CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description

Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1699
Status	New

	Source	Destination
File	freebsd-src-3/e_aes.c	freebsd-src-3/e_aes.c
Line	1491	1491

Object	cipher-	cipher-

Code Snippet
File Name freebsd-src-3/e_aes.c
Method * En/de-crypt plain/cipher-text and authenticate ciphertext. Returns 0 for

```
....
1491.    * En/de-crypt plain/cipher-text and authenticate ciphertext.
Returns 0 for
```

Information Exposure Through Comments\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1700
Status New

	Source	Destination
File	freebsd-src-3/e_aes.c	freebsd-src-3/e_aes.c
Line	1868	1868
Object	cipher-	cipher-

Code Snippet
File Name freebsd-src-3/e_aes.c
Method * authenticated data, en/de-crypt plain/cipher-text and authenticate

```
....
1868.    * authenticated data, en/de-crypt plain/cipher-text and
authenticate
```

Information Exposure Through Comments\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1701
Status New

	Source	Destination
File	freebsd-src-3/e_aes.c	freebsd-src-3/e_aes.c
Line	2043	2043
Object	cipher-	cipher-

Code Snippet
File Name freebsd-src-3/e_aes.c
Method * En/de-crypt plain/cipher-text. Compute tag from plaintext. Returns 0 for

```
....
2043.    * En/de-crypt plain/cipher-text. Compute tag from plaintext.
Returns 0 for
```

Information Exposure Through Comments\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1702
Status	New

	Source	Destination
File	freebsd-src-3/e_aes.c	freebsd-src-3/e_aes.c
Line	2225	2225
Object	cipher-	cipher-

Code Snippet
File Name freebsd-src-3/e_aes.c
Method * authenticated data, en/de-crypt plain/cipher-text and authenticate

```
....
2225.    * authenticated data, en/de-crypt plain/cipher-text and
authenticate
```

Information Exposure Through Comments\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1703
Status	New

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	2570	2570
Object	password (O	password (O

Code Snippet
File Name freebsd-src-3/eap.c
Method * EAP methods can call this function to request open time password (OTP) for

```
....
2570.    * EAP methods can call this function to request open time
password (OTP) for
```

Information Exposure Through Comments\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1704
Status	New

	Source	Destination
File	freebsd-src-3/eap.c	freebsd-src-3/eap.c
Line	2921	2921
Object	password (O	password (O

Code Snippet
File Name freebsd-src-3/eap.c
Method * This function clears a used one-time password (OTP) from the current network

```
....
2921.   * This function clears a used one-time password (OTP) from the
current network
```

Information Exposure Through Comments\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1705
Status	New

	Source	Destination
File	freebsd-src-3/s3_lib.c	freebsd-src-3/s3_lib.c
Line	3180	3180
Object	Cipher-	Cipher-

Code Snippet
File Name freebsd-src-3/s3_lib.c
Method * The list of known Signalling Cipher-Suite Value "ciphers", non-valid

```
....
3180.   * The list of known Signalling Cipher-Suite Value "ciphers",
non-valid
```

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=1060099&projectid=60089&pathid=1670
Status	New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	220	220
Object	f	f

Code Snippet
File Name freebsd-src-3/hxtool.c
Method cms_verify_sd(struct cms_verify_sd_options *opt, int argc, char **argv)

```
....
220.        f = fopen(argv[0], "r");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1671
Status	New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	486	486
Object	f	f

Code Snippet
File Name freebsd-src-3/hxtool.c
Method cms_create_sd(struct cms_create_sd_options *opt, int argc, char **argv)

```
....
486.        f = fopen(outfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1672
Status	New

	Source	Destination
File	freebsd-src-3/hxtool.c	freebsd-src-3/hxtool.c
Line	1107	1107
Object	f	f

Code Snippet
File Name freebsd-src-3/hxtool.c
Method ocsp_fetch(struct ocsp_fetch_options *opt, int argc, char **argv)

```
....
1107.       f = fopen(file, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1673
Status New

	Source	Destination
File	freebsd-src-3/pkinit.c	freebsd-src-3/pkinit.c
Line	1915	1915
Object	f	f

Code Snippet
File Name freebsd-src-3/pkinit.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1915.       f = fopen(fn, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1674
Status New

	Source	Destination
File	freebsd-src-3/t_regex_att.c	freebsd-src-3/t_regex_att.c
Line	394	394
Object	input_file	input_file

Code Snippet
File Name freebsd-src-3/t_regex_att.c
Method att_test(const struct atf_tc *tc, const char *data_name)

```
....
394.        input_file = fopen(data_path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1675
Status New

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	479	479
Object	f	f

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
479.              FILE * f = fopen(data_file, "rb");
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1341
Status New

The size of the buffer used by ldns_rdf_reverse_a in "%s", at line 88 of freebsd-src-3/ldns-host.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ldns_rdf_reverse_a passes to "%s", at line 88 of freebsd-src-3/ldns-host.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c

Line	97	97
Object	"%s"	"%s"

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_rdf_reverse_a(ldns_rdf *addr, const char *base) {

```
....
97.      sprintf(&buf[len], "%s", base);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1342
Status	New

The size of the buffer used by ldns_rdf_reverse_aaaa in "%s", at line 102 of freebsd-src-3/ldns-host.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ldns_rdf_reverse_aaaa passes to "%s", at line 102 of freebsd-src-3/ldns-host.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/ldns-host.c	freebsd-src-3/ldns-host.c
Line	112	112
Object	"%s"	"%s"

Code Snippet
File Name freebsd-src-3/ldns-host.c
Method ldns_rdf_reverse_aaaa(ldns_rdf *addr, const char *base) {

```
....
112.      sprintf(&buf[LDNS_IP6ADDRLEN*4], "%s", base);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1343
Status	New

The size of the buffer used by main in "netmap:%s", at line 2928 of freebsd-src-3/pkt-gen.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to "netmap:%s", at line 2928 of freebsd-src-3/pkt-gen.c, to overwrite the target buffer.

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	3058	3058

Object	"netmap:%s"	"netmap:%s"

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method main(int arc, char **argv)

```
....
3058.                           sprintf(g.ifname, "netmap:%s", optarg);
```

Potential Path Traversal

Query Path:
CPP\Cx\CPP Low Visibility\Potential Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description
Potential Path Traversal\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1029
Status	New

Method main at line 215 of freebsd-src-3/https-client.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 215 of freebsd-src-3/https-client.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	freebsd-src-3/https-client.c	freebsd-src-3/https-client.c
Line	215	479
Object	argv	data_file

Code Snippet
File Name freebsd-src-3/https-client.c
Method main(int argc, char **argv)

```
....
215.  main(int argc, char **argv)
....
479.              FILE * f = fopen(data_file, "rb");
```

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=1060099&projectid=60089&pathid=1344
Status	New

	Source	Destination
File	freebsd-src-3/pkt-gen.c	freebsd-src-3/pkt-gen.c
Line	356	356
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name freebsd-src-3/pkt-gen.c
Method cksum_add(uint16_t sum, uint16_t a)

```
....
356.        return (res + (res < a));
```

Insecure Temporary File

Query Path:
CPP\Cx\CPP Low Visibility\Insecure Temporary File Version:0

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insecure Temporary File\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060099&projectid=60089&pathid=1387
Status	New

	Source	Destination
File	freebsd-src-3/term_tag.c	freebsd-src-3/term_tag.c
Line	110	110
Object	mkstemp	mkstemp

Code Snippet
File Name freebsd-src-3/term_tag.c
Method term_tag_init(const char *outfilename, const char *suffix,

```
....
110.              if ((tfd = mkstemp(tag_files.tfn)) == -1) {
```

Buffer Overflow Indexes

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow OutOfBound

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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
```

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

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

Short 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

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.
An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;

  void setPassword()
```

```
  {
      password = System.console().readLine("Enter your password: ");
   }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed

{
  private SealedObject password;

  void setPassword()

 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
```

```
	gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
	char* password = (char*) malloc(256);
	int i=0;
	char ch;
	ssize_t k;
	while(k = read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n'){
			password[i]='\0';
			break;
		} else{
			password[i++]=ch;
			fflush(0);
		}
	}
	i=0;
	memset(password,'\0',256);
}

int main()

{

	printf("Please enter a password:\n");
	authfunc();
	somefunc();
	char ch;
	while(read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n')
			break;
	}
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of 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

Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obselete since it is relatively easy to break. These obselete algorithms are vulnerable to several different kinds of attacks, including brute force.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.
- Do not use weak, outdated, or obsolete algorithms.
- Ensure you select the correct cryptographic mechanism according to the specific requirements.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
- Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
- Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
- For symmetric encryption, use a key length of at least 256 bits.

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.md5Hex(socialSecurityNum);
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.sha256Hex(socialSecurityNum);
}
```

Use of a One Way Hash without a Salt

Risk

What might happen

If an attacker gains access to the hashed passwords, she would likely be able to reverse the hash due to this weakness, and retrieve the original password. Once the passwords are discovered, the attacker can impersonate the users, and take full advantage of their privileges and access their personal data. Furthermore, this would likely not be discovered, as the attacker is being identified solely by the victims' credentials.

Cause

How does it happen

Typical cryptographic hashes, such as SHA-1 and MD5, are incredibly fast. Combined with attack techniques such as precomputed Rainbow Tables, it is relatively easy for attackers to reverse the hashes, and discover the original passwords. Lack of a unique, random salt added to the password makes brute force attacks even simpler.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.

- Do not use weak, outdated, or obsolete algorithms.

- Ensure you select the correct cryptographic mechanism according to the specific requirements.

Specific Recommendations:

- Passwords should be protected using a password hashing algorithm, instead of a general cryptographic hash. This includes adaptive hashes such as bcrypt, scrypt, PBKDF2 and Argon2.

- Tune the work factor, or cost, of the adaptive hash function according to the designated environment and risk profile.

- Do not use a regular cryptographic hash, such as SHA-1 or MD5, to protect passwords, as these are too fast.

- If it is necessary to use a common hash to protect passwords, add several bytes of unique, random data ("salt") to the password before hashing it. Store the salt with the hashed password, and do not reuse the same salt for multiple passwords.

Source Code Examples

Java

Unsalted Hashed Password

```
private String protectPassword(String password) {
```

```
      byte[] data = password.getBytes();
      byte[] hash = null;

      MessageDigest md = MessageDigest.getInstance("MD5");
      hash = md.digest(data);

      return Base64.getEncoder().encodeToString(hash);
}
```

Fast Hash with Salt

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
            MessageDigest md = MessageDigest.getInstance("SHA-1");

            SecureRandom rand = new SecureRandom();
            byte[] salt = new byte[32];
            rand.nextBytes(salt);

            md.update(salt);
            md.update(data);

            hash = md.digest();
    }
      catch (GeneralSecurityException gse) {
            handleCryptoErrors(gse);
    }
      finally {
            Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

Slow, Adaptive Password Hash

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
            SecureRandom rand = new SecureRandom();
            byte[] salt = new byte[32];
            rand.nextBytes(salt);

            SecretKeyFactory skf = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA512");
            PBEKeySpec spec = new PBEKeySpec(data, salt, ITERATION_COUNT, KEY_LENGTH);
            // ITERATION_COUNT should be configured by environment, KEY_LENGTH should be 256
            SecretKey key = skf.generateSecret(spec);

            hash = key.getEncoded();
    }
      catch (GeneralSecurityException gse) {
            handleCryptoErrors(gse);
    }
      finally {
            Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Wrong Memory Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
```

```
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

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)
```

Potential Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
```

```
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

Reliance on DNS Lookups in a Decision

Risk

What might happen

Relying on reverse DNS records, without verifying domain ownership via cryptographic certificates or protocols, is not a sufficient authentication mechanism. Basing any security decisions on the registered hostname could allow an external attacker to control the application flow. The attacker could possibly perform restricted operations, bypass access controls, and even spoof the user's identity, inject a bogus hostname into the security log, and possibly other logic attacks.

Cause

How does it happen

The application performs a reverse DNS resolution, based on the remote IP address, and performs a security check based on the returned hostname. However, it is relatively easy to spoof DNS names, or cause them to be misreported, depending on the context of the specific environment. If the remote server is controlled by the attacker, it can be configured to report a bogus hostname. Additionally, the attacker could also spoof the hostname if she controls the associated DNS server, or by attacking the legitimate DNS server, or by poisoning the server's DNS cache, or by modifying unprotected DNS traffic to the server. Regardless of the vector, a remote attacker can alter the detected network address, faking the authentication details.

General Recommendations

How to avoid it

- Do not rely on DNS records, network addresses, or system hostnames as a form of authentication, or any other security-related decision.
- Do not perform reverse DNS resolution over an unprotected protocol without record validation.
- Implement a proper authentication mechanism, such as passwords, cryptographic certificates, or public key digital signatures.
- Consider using proposed protocol extensions to cryptographically protect DNS, e.g. DNSSEC (though note the limited support and other drawbacks).

Source Code Examples

Java

Using Reverse DNS as Authentication

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      String ip = req.getRemoteAddr();
      InetAddress address = InetAddress.getByName(ip);

      if (address.getHostName().endsWith(COMPANYNAME)) {
            isCompany = true;
    }
      return isCompany;
```

```
}
```

Verify Authenticated User's Identity

```
private boolean isInternalEmployee(ServletRequest req) {
      boolean isCompany = false;

      Principal user = req.getUserPrincipal();
      if (user != null) {
      if (user.getName().startsWith(COMPANYDOMAIN + "\\")) {
            isCompany = true;
         }
     }
      return isCompany;
}
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names	
Change Date	**Previous Entry Name**
2008-04-11	Code Quality

BACK TO TOP

Use of Obsolete Functions

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

Java

Using Deprecated Methods for Security Checks

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        secManager.checkMulticast(address, 0)
    }

}
```

A Replacement Security Check

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        SocketPermission permission = new SocketPermission(address.getHostAddress(),
"accept,connect");

        secManager.checkPermission(permission)
    }
```

```
}
```

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in

the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

BACK TO TOP

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

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

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	6/19/2024
Common	0105849645654507	6/19/2024