# freebsd-src-2 Scan Report

| | |
|---|---|
| Project Name | freebsd-src-2 |
| Scan Start | Saturday, June 22, 2024 1:59:40 AM |
| Preset | Checkmarx Default |
| Scan Time | 00h:27m:11s |
| Lines Of Code Scanned | 299306 |
| Files Scanned | 151 |
| Report Creation Time | Saturday, June 22, 2024 9:03:30 AM |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088 |
| Team | CxServer |
| Checkmarx Version | 8.7.0 |
| Scan Type | Full |
| Source Origin | LocalPath |
| Density | 5/1000 (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 |

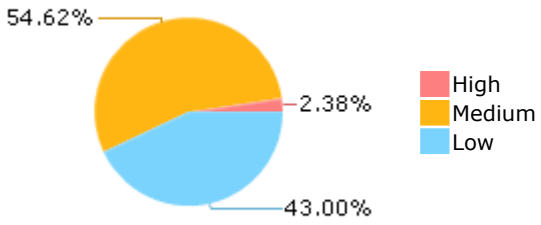
**Results Limit**

Results limit per query was set to 50

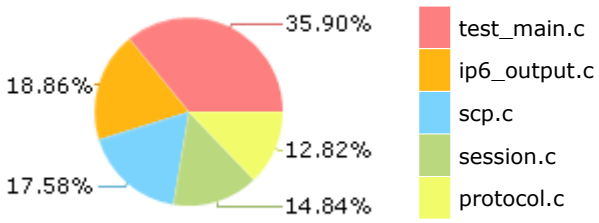
**Selected Queries**

Selected queries are listed in Result Summary

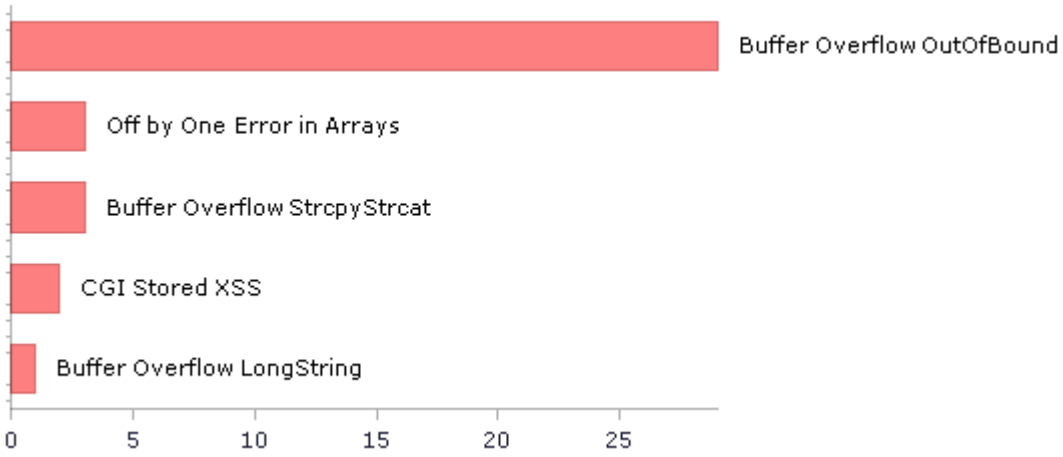
## Result Summary




## 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 | 368 | 219 |
| A2-Broken Authentication | App. Specific | EASY | COMMON | AVERAGE | SEVERE | App. Specific | 188 | 188 |
| A3-Sensitive Data Exposure | App. Specific | AVERAGE | WIDESPREAD | AVERAGE | SEVERE | App. Specific | 14 | 6 |
| 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 | 3 | 2 |
| A6-Security Misconfiguration | App. Specific | EASY | WIDESPREAD | EASY | MODERATE | App. Specific | 0 | 0 |
| A7-Cross-Site Scripting (XSS) | App. Specific | EASY | WIDESPREAD | EASY | MODERATE | App. Specific | 2 | 1 |
| 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 | 360 | 360 |
| 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 | 2 | 1 |
| A4-Insecure Direct Object References | SYSTEM USERS | EASY | COMMON | EASY | MODERATE | EXPOSED DATA | 3 | 2 |
| A5-Security Misconfiguration | EXTERNAL, INTERNAL, ADMIN USERS | EASY | COMMON | EASY | MODERATE | ALL DATA AND SYSTEM | 0 | 0 |
| A6-Sensitive Data Exposure | EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS | DIFFICULT | UNCOMMON | AVERAGE | SEVERE | EXPOSED DATA | 13 | 5 |
| A7-Missing Function Level Access Control* | EXTERNAL, INTERNAL USERS | EASY | COMMON | AVERAGE | MODERATE | EXPOSED DATA AND FUNCTIONS | 0 | 0 |
| A8-Cross-Site Request Forgery (CSRF) | USERS BROWSERS | AVERAGE | COMMON | EASY | MODERATE | AFFECTED DATA AND FUNCTIONS | 0 | 0 |
| A9-Using Components with Known Vulnerabilities* | EXTERNAL USERS, AUTOMATED TOOLS | AVERAGE | WIDESPREAD | DIFFICULT | MODERATE | AFFECTED DATA AND FUNCTIONS | 360 | 360 |
| 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 | 3 | 3 |
| PCI DSS (3.2) - 6.5.2 - Buffer overflows | 225 | 201 |
| 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) | 2 | 1 |
| 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. | 37 | 37 |
| 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. | 4 | 4 |
| 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. | 39 | 39 |
| 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. | 159 | 154 |
| 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. | 7 | 4 |
| 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. | 27 | 26 |

***** 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) | 227 | 227 |
| AC-4 Information Flow Enforcement (P1) | 0 | 0 |
| AC-6 Least Privilege (P1) | 0 | 0 |
| AU-9 Protection of Audit Information (P1) | 0 | 0 |
| CM-6 Configuration Settings (P2) | 0 | 0 |
| IA-5 Authenticator Management (P1) | 0 | 0 |
| IA-6 Authenticator Feedback (P2) | 0 | 0 |
| IA-8 Identification and Authentication (Non-Organizational Users) (P1) | 0 | 0 |
| SC-12 Cryptographic Key Establishment and Management (P1) | 0 | 0 |
| SC-13 Cryptographic Protection (P1) | 0 | 0 |
| SC-17 Public Key Infrastructure Certificates (P1) | 0 | 0 |
| SC-18 Mobile Code (P2) | 0 | 0 |
| SC-23 Session Authenticity (P1)* | 1 | 1 |
| SC-28 Protection of Information at Rest (P1) | 1 | 1 |
| SC-4 Information in Shared Resources (P1) | 14 | 6 |
| SC-5 Denial of Service Protection (P1)* | 332 | 145 |
| SC-8 Transmission Confidentiality and Integrity (P1) | 0 | 0 |
| SI-10 Information Input Validation (P1)* | 82 | 58 |
| SI-11 Error Handling (P2)* | 102 | 102 |
| SI-15 Information Output Filtering (P0) | 2 | 1 |
| SI-16 Memory Protection (P1) | 27 | 19 |

***** 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:<br>-Failing to identify the user at all when that should be required<br>-Failure to maintain the user's identity when it is required<br>-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.).<br>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 |

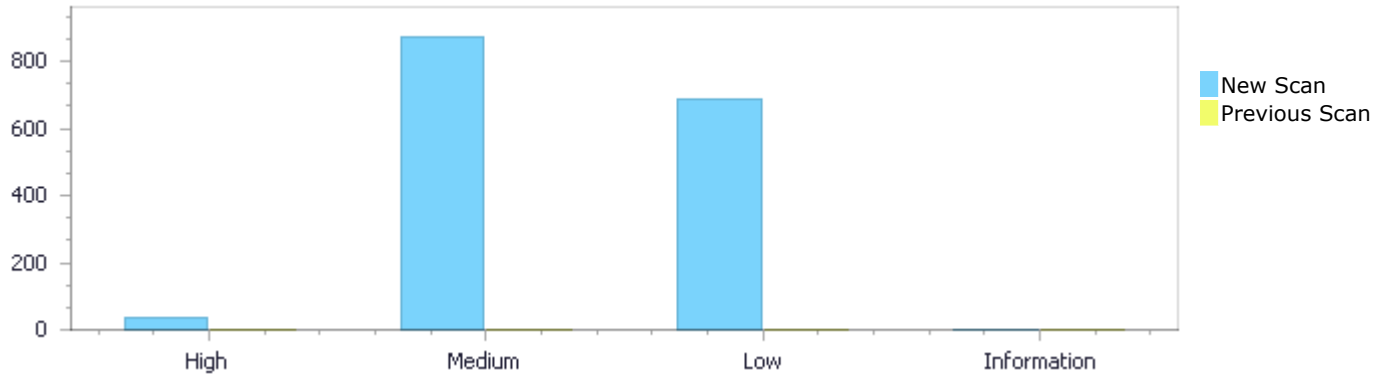
# Scan Summary - Custom

| 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 | 38 | 874 | 688 | 0 | 1,600 |
| Recurrent Issues | 0 | 0 | 0 | 0 | 0 |
| Total | 38 | 874 | 688 | 0 | 1,600 |
| | | | | | |
| 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 | 38 | 874 | 688 | 0 | 1,600 |
| Urgent | 0 | 0 | 0 | 0 | 0 |
| Proposed Not Exploitable | 0 | 0 | 0 | 0 | 0 |
| Total | 38 | 874 | 688 | 0 | 1,600 |

## Result Summary

| Vulnerability Type | Occurrences | Severity |
|---|---|---|
| Buffer Overflow OutOfBound | 29 | High |
| Buffer Overflow StrcpyStrcat | 3 | High |
| Off by One Error in Arrays | 3 | High |
| CGI Stored XSS | 2 | High |
| Buffer Overflow LongString | 1 | High |

| | | |
|---|---|---|
| Dangerous Functions | 313 | Medium |
| Buffer Overflow boundcpy WrongSizeParam | 156 | Medium |
| MemoryFree on StackVariable | 147 | Medium |
| Use of Zero Initialized Pointer | 75 | Medium |
| Memory Leak | 45 | Medium |
| Wrong Size t Allocation | 33 | Medium |
| Integer Overflow | 25 | Medium |
| Double Free | 21 | Medium |
| Use of Uninitialized Variable | 21 | Medium |
| Use of Uninitialized Pointer | 19 | Medium |
| Heap Inspection | 7 | Medium |
| Divide By Zero | 4 | Medium |
| Char Overflow | 3 | Medium |
| Path Traversal | 3 | Medium |
| Buffer Overflow AddressOfLocalVarReturned | 2 | Medium |
| NULL Pointer Dereference | 166 | Low |
| Improper Resource Access Authorization | 151 | Low |
| Unchecked Return Value | 102 | Low |
| Use of Sizeof On a Pointer Type | 52 | Low |
| Use of Obsolete Functions | 47 | Low |
| Exposure of System Data to Unauthorized Control Sphere | 39 | Low |
| Incorrect Permission Assignment For Critical Resources | 37 | Low |
| TOCTOU | 27 | Low |
| Sizeof Pointer Argument | 24 | Low |
| Unchecked Array Index | 16 | Low |
| Inconsistent Implementations | 6 | Low |
| Privacy Violation | 6 | Low |
| Arithmenic Operation On Boolean | 4 | Low |
| Heuristic 2nd Order Buffer Overflow read | 3 | Low |
| Potential Off by One Error in Loops | 3 | Low |
| Potential Precision Problem | 2 | Low |
| Information Exposure Through Comments | 1 | Low |
| Insecure Temporary File | 1 | Low |
| Reliance on DNS Lookups in a Decision | 1 | Low |

# 10 Most Vulnerable Files

## High and Medium Vulnerabilities

| File Name | Issues Found |
|---|---|
| freebsd-src-2/test_main.c | 100 |
| freebsd-src-2/protocol.c | 68 |
| freebsd-src-2/scp.c | 67 |
| freebsd-src-2/wlan_sys.c | 49 |
| freebsd-src-2/buffer.c | 37 |
| freebsd-src-2/rtsol.c | 31 |
| freebsd-src-2/X86_64.cpp | 31 |
| freebsd-src-2/cachedump.c | 30 |
| freebsd-src-2/rec_layer_d1.c | 29 |
| freebsd-src-2/ext2_extents.c | 28 |

# 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=1060098&projectid=60088&pathid=8 |
| Status | New |

The size of the buffer used by response in cp, at line 2057 of freebsd-src-2/scp.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that response passes to cp, at line 2057 of freebsd-src-2/scp.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 2080 | 2080 |
| Object | cp | cp |

Code Snippet
File Name freebsd-src-2/scp.c
Method response(void)

```
....
2080.                    cp[-1] = '\0';
```

**Buffer Overflow OutOfBound\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=9 |
| Status | New |

The size of the buffer used by bwi_rf_get_gains in i, at line 373 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_get_gains passes to save_rf, at line 373 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |

| | | |
|---|---|---|
| Line | 391 | 505 |
| Object | save_rf | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_get_gains(struct bwi_mac *mac)

```
....
391.        uint16_t save_rf[SAVE_RF_MAX];
....
505.              RF_WRITE(mac, save_rf_regs[i], save_rf[i]);
```

**Buffer Overflow OutOfBound\Path 3:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=10
Status New

The size of the buffer used by bwi_rf_get_gains in i, at line 373 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_get_gains passes to save_rf, at line 373 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 391 | 403 |
| Object | save_rf | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_get_gains(struct bwi_mac *mac)

```
....
391.        uint16_t save_rf[SAVE_RF_MAX];
....
403.              save_rf[i] = RF_READ(mac, save_rf_regs[i]);
```

**Buffer Overflow OutOfBound\Path 4:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=11
Status New

The size of the buffer used by bwi_rf_get_gains in i, at line 373 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_get_gains passes to save_rf_regs, at line 373 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 378 | 505 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_get_gains(struct bwi_mac *mac)

```
....
378.        static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
505.                RF_WRITE(mac, save_rf_regs[i], save_rf[i]);
```

**Buffer Overflow OutOfBound\Path 5:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=12
Status New

The size of the buffer used by bwi_rf_get_gains in i, at line 373 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_get_gains passes to save_rf_regs, at line 373 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 378 | 403 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_get_gains(struct bwi_mac *mac)

```
....
378.        static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
403.                save_rf[i] = RF_READ(mac, save_rf_regs[i]);
```

**Buffer Overflow OutOfBound\Path 6:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=13
Status New

The size of the buffer used by bwi_rf_get_gains in i, at line 373 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_get_gains passes to save_rf_regs, at line 373 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 378 | 403 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_get_gains(struct bwi_mac *mac)

```
....
378.        static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
403.                save_rf[i] = RF_READ(mac, save_rf_regs[i]);
```

**Buffer Overflow OutOfBound\Path 7:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=14
Status New

The size of the buffer used by bwi_rf_get_gains in i, at line 373 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_get_gains passes to save_rf_regs, at line 373 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 378 | 505 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_get_gains(struct bwi_mac *mac)

```
....
378.        static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
505.                RF_WRITE(mac, save_rf_regs[i], save_rf[i]);
```

**Buffer Overflow OutOfBound\Path 8:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=15
Status New

The size of the buffer used by bwi_rf_set_nrssi_ofs_11g in i, at line 1750 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that bwi_rf_set_nrssi_ofs_11g passes to save_rf, at line 1750 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1769 | 1881 |
| Object | save_rf | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_set_nrssi_ofs_11g(struct bwi_mac *mac)

```
....
1769.       uint16_t save_rf[SAVE_RF_MAX];
....
1881.               RF_WRITE(mac, save_rf_regs[i], save_rf[i]);
```

**Buffer Overflow OutOfBound\Path 9:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=16
Status New

The size of the buffer used by bwi_rf_set_nrssi_ofs_11g in i, at line 1750 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_set_nrssi_ofs_11g passes to save_rf, at line 1750 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1769 | 1779 |
| Object | save_rf | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_set_nrssi_ofs_11g(struct bwi_mac *mac)

```
....
1769.       uint16_t save_rf[SAVE_RF_MAX];
....
1779.               save_rf[i] = RF_READ(mac, save_rf_regs[i]);
```

**Buffer Overflow OutOfBound\Path 10:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=17
Status New

The size of the buffer used by bwi_rf_set_nrssi_ofs_11g in i, at line 1750 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_set_nrssi_ofs_11g passes to save_rf_regs, at line 1750 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1756 | 1881 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_set_nrssi_ofs_11g(struct bwi_mac *mac)

```
....
1756.       static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
1881.             RF_WRITE(mac, save_rf_regs[i], save_rf[i]);
```

**Buffer Overflow OutOfBound\Path 11:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=18
Status New

The size of the buffer used by bwi_rf_set_nrssi_ofs_11g in i, at line 1750 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_set_nrssi_ofs_11g passes to save_rf_regs, at line 1750 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1756 | 1779 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_set_nrssi_ofs_11g(struct bwi_mac *mac)

```
....
1756.       static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
1779.             save_rf[i] = RF_READ(mac, save_rf_regs[i]);
```

**Buffer Overflow OutOfBound\Path 12:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=19 |
| Status | New |

The size of the buffer used by bwi_rf_set_nrssi_ofs_11g in i, at line 1750 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_set_nrssi_ofs_11g passes to save_rf_regs, at line 1750 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1756 | 1779 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_set_nrssi_ofs_11g(struct bwi_mac *mac)

```
....
1756.       static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
1779.             save_rf[i] = RF_READ(mac, save_rf_regs[i]);
```

**Buffer Overflow OutOfBound\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=20 |
| Status | New |

The size of the buffer used by bwi_rf_set_nrssi_ofs_11g in i, at line 1750 of freebsd-src-2/bwirf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bwi_rf_set_nrssi_ofs_11g passes to save_rf_regs, at line 1750 of freebsd-src-2/bwirf.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1756 | 1881 |
| Object | save_rf_regs | i |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_set_nrssi_ofs_11g(struct bwi_mac *mac)

```
....
1756.       static const uint16_t save_rf_regs[SAVE_RF_MAX] =
....
1881.             RF_WRITE(mac, save_rf_regs[i], save_rf[i]);
```

**Buffer Overflow OutOfBound\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=21 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in l_pid, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to pid, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 870 | 927 |
| Object | pid | l_pid |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
870.        pid_t pid[5];
....
927.                    result[nlocks].l_pid = pid[i];
```

**Buffer Overflow OutOfBound\Path 15:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=22 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in nlocks, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to pid, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 870 | 926 |
| Object | pid | nlocks |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
870.        pid_t pid[5];
....
926.                    result[nlocks] = lock[i];
```

**Buffer Overflow OutOfBound\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=23 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in l_pid, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to fd, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 869 | 927 |
| Object | fd | l_pid |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
869.        int fd[5];
....
927.                    result[nlocks].l_pid = pid[i];
```

**Buffer Overflow OutOfBound\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=24 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in nlocks, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to fd, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 869 | 926 |
| Object | fd | nlocks |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
869.        int fd[5];
....
926.                    result[nlocks] = lock[i];
```

**Buffer Overflow OutOfBound\Path 18:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=25 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in l_pid, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to lock, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 858 | 927 |
| Object | lock | l_pid |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
858.        const struct flock lock[4] = {
....
927.                    result[nlocks].l_pid = pid[i];
```

**Buffer Overflow OutOfBound\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=26 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in nlocks, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to lock, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 858 | 926 |

| | | |
|---|---|---|
| Object | lock | nlocks |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
858.        const struct flock lock[4] = {
....
926.                    result[nlocks] = lock[i];
```

**Buffer Overflow OutOfBound\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=27 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in l_pid, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to result, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 866 | 927 |
| Object | result | l_pid |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
866.        struct flock result[5];
....
927.                    result[nlocks].l_pid = pid[i];
```

**Buffer Overflow OutOfBound\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=28 |
| Status | New |

The size of the buffer used by fcntl_getlock_pids in nlocks, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to result, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 866 | 926 |
| Object | result | nlocks |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
866.        struct flock result[5];
....
926.                    result[nlocks] = lock[i];
```

**Buffer Overflow OutOfBound\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=29 |
| Status | New |

The size of the buffer used by probe_adapters in i, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1167 |
| Object | biosadapter | i |

Code Snippet
File Name freebsd-src-2/vga.c
Method static video_adapter_t biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c
Method probe_adapters(void)

```
....
1167.           clear_mode_map(&biosadapter[i], mode_map, M_VGA_CG320 +
1,
```

**Buffer Overflow OutOfBound\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=30 |
| Status | New |

The size of the buffer used by probe_adapters in i, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1165 |
| Object | biosadapter | i |

Code Snippet

File Name freebsd-src-2/vga.c

Method static video_adapter_t biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c

Method probe_adapters(void)

```
....
1165.           if (!(biosadapter[i].va_flags & V_ADP_MODECHANGE))
```

**Buffer Overflow OutOfBound\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=31 |
| Status | New |

The size of the buffer used by probe_adapters in biosadapter, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1168 |
| Object | biosadapter | biosadapter |

Code Snippet

File Name freebsd-src-2/vga.c

Method static video_adapter_t biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c

Method probe_adapters(void)

```
....
1168.                       (biosadapter[i].va_flags & V_ADP_COLOR) ?
```

**Buffer Overflow OutOfBound\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=32 |
| Status | New |

The size of the buffer used by probe_adapters in i, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1170 |
| Object | biosadapter | i |

Code Snippet

File Name freebsd-src-2/vga.c

Method static video_adapter_t  biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c

Method probe_adapters(void)

```
....
1170.           if ((biosadapter[i].va_type == KD_VGA)
```

**Buffer Overflow OutOfBound\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=33 |
| Status | New |

The size of the buffer used by probe_adapters in i, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1171 |
| Object | biosadapter | i |

Code Snippet
File Name freebsd-src-2/vga.c
Method static video_adapter_t biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c
Method probe_adapters(void)

```
....
1171.             || (biosadapter[i].va_type == KD_EGA)) {
```

**Buffer Overflow OutOfBound\Path 27:**

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=34
Status New

The size of the buffer used by probe_adapters in va_io_base, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1172 |
| Object | biosadapter | va_io_base |

Code Snippet
File Name freebsd-src-2/vga.c
Method static video_adapter_t biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c

Method probe_adapters(void)

```
....
1172.              biosadapter[i].va_io_base =
```

**Buffer Overflow OutOfBound\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=35 |
| Status | New |

The size of the buffer used by probe_adapters in i, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1173 |
| Object | biosadapter | i |

Code Snippet

File Name freebsd-src-2/vga.c

Method static video_adapter_t biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c

Method probe_adapters(void)

```
....
1173.                (biosadapter[i].va_flags & V_ADP_COLOR) ?
```

**Buffer Overflow OutOfBound\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=36 |
| Status | New |

The size of the buffer used by probe_adapters in va_io_size, at line 891 of freebsd-src-2/vga.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that

video_adapter_t biosadapter[2]; passes to biosadapter, at line 192 of freebsd-src-2/vga.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 192 | 1175 |
| Object | biosadapter | va_io_size |

Code Snippet
File Name freebsd-src-2/vga.c
Method static video_adapter_t biosadapter[2];

```
....
192.  static video_adapter_t  biosadapter[2];
```

File Name freebsd-src-2/vga.c
Method probe_adapters(void)

```
....
1175.              biosadapter[i].va_io_size = 32;
```

## Off by One Error in Arrays

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Arrays Version:0

### 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*
**Off by One Error in Arrays\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=2 |
| Status | New |

The buffer allocated by sizeof in freebsd-src-2/telnet.c at line 1295 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-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1295 | 1295 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c

| | |
|---|---|
| Method | unsigned char const * const slc_reply_eom = &slc_reply[sizeof(slc_reply)]; |

```
....
1295.  unsigned char const * const slc_reply_eom =
&slc_reply[sizeof(slc_reply)];
```

**Off by One Error in Arrays\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=3 |
| Status | New |

The buffer allocated by sizeof in freebsd-src-2/respip.c at line 567 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-2/respip.c | freebsd-src-2/respip.c |
| Line | 579 | 579 |
| Object | sizeof | sizeof |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/respip.c |
| Method | rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i, |

```
....
579.              *addrlenp = sizeof(*sa4);
```

**Off by One Error in Arrays\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=4 |
| Status | New |

The buffer allocated by sizeof in freebsd-src-2/respip.c at line 567 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-2/respip.c | freebsd-src-2/respip.c |
| Line | 588 | 588 |
| Object | sizeof | sizeof |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/respip.c |
| Method | rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i, |

```
....
588.              *addrlenp = sizeof(*sa6);
```

## 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=1060098&projectid=60088&pathid=5 |
| Status | New |

The size of the buffer used by realloc_strcat in new_str, at line 189 of freebsd-src-2/subst.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that realloc_strcat passes to str, at line 189 of freebsd-src-2/subst.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/subst.c | freebsd-src-2/subst.c |
| Line | 189 | 204 |
| Object | str | new_str |

Code Snippet
File Name freebsd-src-2/subst.c
Method realloc_strcat(char **str, const char *append)

```
....
189.  realloc_strcat(char **str, const char *append)
....
204.        strcpy(new_str + old_len, append);
```

**Buffer Overflow StrcpyStrcat\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=6 |
| Status | New |

The size of the buffer used by realloc_strcat in BinaryExpr, at line 189 of freebsd-src-2/subst.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that realloc_strcat passes to str, at line 189 of freebsd-src-2/subst.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/subst.c | freebsd-src-2/subst.c |
| Line | 189 | 204 |
| Object | str | BinaryExpr |

Code Snippet
File Name freebsd-src-2/subst.c
Method realloc_strcat(char **str, const char *append)

```
....
189.  realloc_strcat(char **str, const char *append)
....
204.        strcpy(new_str + old_len, append);
```

**Buffer Overflow StrcpyStrcat\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=7 |
| Status | New |

The size of the buffer used by lookup_simple in mountpath, at line 67 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lookup_simple passes to mountpath, at line 67 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 67 | 72 |
| Object | mountpath | mountpath |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method lookup_simple(const atf_tc_t *tc, const char *mountpath)

```
....
67.  lookup_simple(const atf_tc_t *tc, const char *mountpath)
....
72.   strcpy(final, mountpath);
```

## CGI Stored XSS

Query Path:
CPP\Cx\CPP High Risk\CGI Stored XSS Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)

*Description*

**CGI Stored XSS\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=195 |
| Status | New |

Unvalidated DB output was found in line number 115 in freebsd-src-2/maketab.c file. A possible XSS exploitation was found in printf at line number 115.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 138 | 170 |
| Object | buf | printf |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
138.        while (fgets(buf, sizeof buf, fp) != NULL) {
....
170.              printf("\t\"%s\",\t/* %d */\n", name, tok);
```

**CGI Stored XSS\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=196 |
| Status | New |

Unvalidated DB output was found in line number 115 in freebsd-src-2/maketab.c file. A possible XSS exploitation was found in printf at line number 115.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 138 | 179 |
| Object | buf | printf |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
138.        while (fgets(buf, sizeof buf, fp) != NULL) {
....
179.              printf("\t%s,\t/* %s */\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=1060098&projectid=60088&pathid=1 |
| Status | New |

The size of the buffer used by rsource in vect, at line 1490 of freebsd-src-2/scp.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rsource passes to "%s/%s", at line 1490 of freebsd-src-2/scp.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1529 | 1530 |
| Object | "%s/%s" | vect |

Code Snippet
File Name freebsd-src-2/scp.c
Method rsource(char *name, struct stat *statp)

```
....
1529.               (void) snprintf(path, sizeof path, "%s/%s", name, dp-
>d_name);
1530.               vect[0] = path;
```

## 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=1060098&projectid=60088&pathid=427 |
| Status | New |

The dangerous function, memcpy, was found in use at line 387 in freebsd-src-2/a_int.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/a_int.c | freebsd-src-2/a_int.c |
| Line | 431 | 431 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/a_int.c
Method ASN1_INTEGER *d2i_ASN1_UINTEGER(ASN1_INTEGER **a, const unsigned char **pp,

```
....
431.          memcpy(s, p, (int)len);
```

**Dangerous Functions\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=428
Status New

The dangerous function, memcpy, was found in use at line 21 in freebsd-src-2/a_object.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/a_object.c | freebsd-src-2/a_object.c |
| Line | 43 | 43 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/a_object.c
Method int i2d_ASN1_OBJECT(const ASN1_OBJECT *a, unsigned char **pp)

```
....
43.       memcpy(p, a->data, a->length);
```

**Dangerous Functions\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=429
Status New

The dangerous function, memcpy, was found in use at line 239 in freebsd-src-2/a_object.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/a_object.c | freebsd-src-2/a_object.c |
| Line | 312 | 312 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/a_object.c
Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
312.      memcpy(data, p, length);
```

**Dangerous Functions\Path 4:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=430
Status New

The dangerous function, memcpy, was found in use at line 809 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 837 | 837 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method PRESERVE_PINNED(struct evbuffer *src, struct evbuffer_chain **first,

```
....
837.              memcpy(tmp->buffer, chain->buffer + chain->misalign,
```

**Dangerous Functions\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=431
Status New

The dangerous function, memcpy, was found in use at line 1185 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1226 | 1226 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_copyout_from(struct evbuffer *buf, const struct evbuffer_ptr *pos,

```
....
1226.             memcpy(data,
```

**Dangerous Functions\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=432 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1185 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1241 | 1241 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_copyout_from(struct evbuffer *buf, const struct evbuffer_ptr *pos,

```
....
1241.             memcpy(data, chain->buffer + chain->misalign +
pos_in_chain,
```

**Dangerous Functions\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=433 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1345 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |

| | | |
|---|---|---|
| Line | 1419 | 1419 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_pullup(struct evbuffer *buf, ev_ssize_t size)

```
....
1419.             memcpy(buffer, chain->buffer + chain->misalign, chain-
>off);
```

**Dangerous Functions\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=434 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1345 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1431 | 1431 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_pullup(struct evbuffer *buf, ev_ssize_t size)

```
....
1431.             memcpy(buffer, chain->buffer + chain->misalign, size);
```

**Dangerous Functions\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=435 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1590 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1609 | 1609 |

| | | |
|---|---|---|
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_search_eol(struct evbuffer *buffer,

```
....
1609.             memcpy(&it, start, sizeof(it));
```

**Dangerous Functions\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=436 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1590 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1622 | 1622 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_search_eol(struct evbuffer *buffer,

```
....
1622.             memcpy(&it2, &it, sizeof(it));
```

**Dangerous Functions\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=437 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1590 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1644 | 1644 |
| Object | memcpy | memcpy |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_search_eol(struct evbuffer *buffer, |

```
....
1644.             memcpy(&it2, &it, sizeof(it));
```

**Dangerous Functions\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=438 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1590 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1648 | 1648 |
| Object | memcpy | memcpy |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_search_eol(struct evbuffer *buffer, |

```
....
1648.                   memcpy(&it, &it2, sizeof(it));
```

**Dangerous Functions\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=439 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1723 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1763 | 1763 |
| Object | memcpy | memcpy |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_add(struct evbuffer *buf, const void *data_in, size_t datlen) |

```
....
1763.                    memcpy(chain->buffer + chain->misalign + chain-
>off,
```

**Dangerous Functions\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=440 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1723 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1774 | 1774 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_add(struct evbuffer *buf, const void *data_in, size_t datlen)

```
....
1774.                    memcpy(chain->buffer + chain->off, data,
datlen);
```

**Dangerous Functions\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=441 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1723 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1796 | 1796 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_add(struct evbuffer *buf, const void *data_in, size_t datlen)

```
....
1796.             memcpy(chain->buffer + chain->misalign + chain->off,
```

**Dangerous Functions\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=442 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1723 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1806 | 1806 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_add(struct evbuffer *buf, const void *data_in, size_t datlen)

```
....
1806.       memcpy(tmp->buffer, data, datlen);
```

**Dangerous Functions\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=443 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1820 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1856 | 1856 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_prepend(struct evbuffer *buf, const void *data, size_t datlen)

```
....
1856.                    memcpy(chain->buffer + chain->misalign - datlen,
```

**Dangerous Functions\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=444 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1820 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1865 | 1865 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_prepend(struct evbuffer *buf, const void *data, size_t datlen)

```
....
1865.                    memcpy(chain->buffer,
```

**Dangerous Functions\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=445 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1820 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1889 | 1889 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_prepend(struct evbuffer *buf, const void *data, size_t datlen)

```
....
1889.       memcpy(tmp->buffer + tmp->misalign, data, datlen);
```

**Dangerous Functions\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=446 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1928 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 2012 | 2012 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_expand_singlechain(struct evbuffer *buf, size_t datlen)

```
....
2012.             memcpy(tmp->buffer, chain->buffer + chain->misalign,
```

**Dangerous Functions\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=447 |
| Status | New |

The dangerous function, memcpy, was found in use at line 2708 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 2718 | 2718 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_search_range(struct evbuffer *buffer, const char *what, size_t len, const struct evbuffer_ptr *start, const struct evbuffer_ptr *end)

```
....
2718.             memcpy(&pos, start, sizeof(pos));
```

**Dangerous Functions\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=448 |
| Status | New |

The dangerous function, memcpy, was found in use at line 2831 in freebsd-src-2/buffer.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 2863 | 2863 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_add_vprintf(struct evbuffer *buf, const char *fmt, va_list ap)

```
....
2863.             va_copy(aq, ap);
```

**Dangerous Functions\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=449 |
| Status | New |

The dangerous function, memcpy, was found in use at line 85 in freebsd-src-2/cap_sendmsg.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cap_sendmsg.c | freebsd-src-2/cap_sendmsg.c |
| Line | 120 | 120 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/cap_sendmsg.c
Method sendpacket(int sock, struct sockaddr_in6 *dst, uint32_t ifindex, int hoplimit,

```
....
120.        memcpy(CMSG_DATA(cm), &hoplimit, sizeof(int));
```

**Dangerous Functions\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=450 |
| Status | New |

The dangerous function, memcpy, was found in use at line 388 in freebsd-src-2/cut.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cut.c | freebsd-src-2/cut.c |
| Line | 406 | 406 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/cut.c
Method f_cut(FILE *fp, const char *fname)

```
....
406.                    memcpy(mlbuf, lbuf, lbuflen);
```

**Dangerous Functions\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=451 |
| Status | New |

The dangerous function, memcpy, was found in use at line 287 in freebsd-src-2/d1_lib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/d1_lib.c | freebsd-src-2/d1_lib.c |
| Line | 308 | 308 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/d1_lib.c
Method struct timeval *dtls1_get_timeout(SSL *s, struct timeval *timeleft)

```
....
308.      memcpy(timeleft, &(s->d1->next_timeout), sizeof(struct
timeval));
```

**Dangerous Functions\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=452 |
| Status | New |

The dangerous function, memcpy, was found in use at line 446 in freebsd-src-2/d1_lib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/d1_lib.c | freebsd-src-2/d1_lib.c |
| Line | 776 | 776 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/d1_lib.c
Method int DTLSv1_listen(SSL *s, BIO_ADDR *client)

```
....
776.              memcpy(&wbuf[DTLS1_RT_HEADER_LENGTH + 1],
```

**Dangerous Functions\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=453 |
| Status | New |

The dangerous function, memcpy, was found in use at line 207 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 240 | 240 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
240.              memcpy(gctx->iv, iv, gctx->ivlen);
```

**Dangerous Functions\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=454 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 284 | 284 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
284.          memcpy(EVP_CIPHER_CTX_buf_noconst(c), ptr, arg);
```

**Dangerous Functions\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=455 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 292 | 292 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
292.          memcpy(ptr, EVP_CIPHER_CTX_buf_noconst(c), arg);
```

**Dangerous Functions\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=456 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 298 | 298 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
298.              memcpy(gctx->iv, ptr, gctx->ivlen);
```

**Dangerous Functions\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=457 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 309 | 309 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
309.              memcpy(gctx->iv, ptr, arg);
```

**Dangerous Functions\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=458 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 322 | 322 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
322.          memcpy(ptr, gctx->iv + gctx->ivlen - arg, arg);
```

**Dangerous Functions\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=459 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 335 | 335 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
335.          memcpy(gctx->iv + gctx->ivlen - arg, ptr, arg);
```

**Dangerous Functions\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=460 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 344 | 344 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
344.          memcpy(EVP_CIPHER_CTX_buf_noconst(c), ptr, arg);
```

**Dangerous Functions\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=461 |
| Status | New |

The dangerous function, memcpy, was found in use at line 247 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 382 | 382 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
382.                    memcpy(gctx_out->iv, gctx->iv, gctx->ivlen);
```

**Dangerous Functions\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=462 |
| Status | New |

The dangerous function, memcpy, was found in use at line 503 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 525 | 525 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_ccm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
525.            memcpy(EVP_CIPHER_CTX_iv_noconst(ctx), iv, 15 - cctx->L);
```

**Dangerous Functions\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=463 |
| Status | New |

The dangerous function, memcpy, was found in use at line 531 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 550 | 550 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_ccm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
550.          memcpy(EVP_CIPHER_CTX_buf_noconst(c), ptr, arg);
```

**Dangerous Functions\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=464 |
| Status | New |

The dangerous function, memcpy, was found in use at line 531 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 577 | 577 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_ccm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
577.          memcpy(EVP_CIPHER_CTX_iv_noconst(c), ptr, arg);
```

**Dangerous Functions\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=465 |
| Status | New |

The dangerous function, memcpy, was found in use at line 531 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 599 | 599 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_ccm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
599.              memcpy(EVP_CIPHER_CTX_buf_noconst(c), ptr, arg);
```

**Dangerous Functions\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=466 |
| Status | New |

The dangerous function, memcpy, was found in use at line 631 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 642 | 642 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_ccm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
642.          memcpy(out, EVP_CIPHER_CTX_buf_noconst(ctx),
```

**Dangerous Functions\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=467 |
| Status | New |

The dangerous function, memcpy, was found in use at line 631 in freebsd-src-2/e_aria.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 645 | 645 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_ccm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
645.      memcpy(EVP_CIPHER_CTX_iv_noconst(ctx) +
EVP_CCM_TLS_FIXED_IV_LEN, in,
```

**Dangerous Functions\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=468 |
| Status | New |

The dangerous function, memcpy, was found in use at line 65 in freebsd-src-2/e_rc4_hmac_md5.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_rc4_hmac_md5.c | freebsd-src-2/e_rc4_hmac_md5.c |
| Line | 112 | 112 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_rc4_hmac_md5.c
Method static int rc4_hmac_md5_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
112.                    memcpy(out + rc4_off, in + rc4_off, plen -
rc4_off);
```

**Dangerous Functions\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=469 |
| Status | New |

The dangerous function, memcpy, was found in use at line 176 in freebsd-src-2/e_rc4_hmac_md5.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/e_rc4_hmac_md5.c | freebsd-src-2/e_rc4_hmac_md5.c |
| Line | 194 | 194 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/e_rc4_hmac_md5.c
Method static int rc4_hmac_md5_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

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

**Dangerous Functions\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=470 |
| Status | New |

The dangerous function, memcpy, was found in use at line 550 in freebsd-src-2/ext2_extents.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 558 | 558 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_fill_path_bdata(struct ext4_extent_path *path,

```
....
558.        memcpy(path->ep_data, bp->b_data, bp->b_bufsize);
```

**Dangerous Functions\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=471 |
| Status | New |

The dangerous function, memcpy, was found in use at line 565 in freebsd-src-2/ext2_extents.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 571 | 571 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_fill_path_buf(struct ext4_extent_path *path, struct buf *bp)

```
....
571.        memcpy(bp->b_data, path->ep_data, bp->b_bufsize);
```

**Dangerous Functions\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=472 |
| Status | New |

The dangerous function, memcpy, was found in use at line 159 in freebsd-src-2/http-server.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 236 | 236 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/http-server.c
Method send_document_cb(struct evhttp_request *req, void *arg)

```
....
236.              memcpy(pattern, whole_path, dirlen);
```

**Dangerous Functions\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=473 |
| Status | New |

The dangerous function, memcpy, was found in use at line 331 in freebsd-src-2/init.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/init.c | freebsd-src-2/init.c |
| Line | 340 | 340 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/init.c
Method mt7615_regd_notifier(struct wiphy *wiphy,

```
....
340.        memcpy(dev->mt76.alpha2, request->alpha2, sizeof(dev-
>mt76.alpha2));
```

**Dangerous Functions\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=474 |
| Status | New |

The dangerous function, memcpy, was found in use at line 446 in freebsd-src-2/init.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/init.c | freebsd-src-2/init.c |
| Line | 487 | 487 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/init.c
Method int mt7615_register_ext_phy(struct mt7615_dev *dev)

```
....
487.        memcpy(mphy->macaddr, dev->mt76.eeprom.data +
MT_EE_MAC_ADDR,
```

**Dangerous Functions\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=475 |
| Status | New |

The dangerous function, memcpy, was found in use at line 174 in freebsd-src-2/ips_commands.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ips_commands.c | freebsd-src-2/ips_commands.c |
| Line | 202 | 202 |
| Object | memcpy | memcpy |

Code Snippet
File Name freebsd-src-2/ips_commands.c
Method static void ips_adapter_info_callback(void *cmdptr, bus_dma_segment_t *segments,int segnum, int error)

```
....
202.        memcpy(&(sc->adapter_info), command->data_buffer,
IPS_ADAPTER_INFO_LEN);
```

**Dangerous Functions\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=476 |
| Status | New |

The dangerous function, memcpy, was found in use at line 273 in freebsd-src-2/ips_commands.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ips_commands.c | freebsd-src-2/ips_commands.c |
| Line | 304 | 304 |
| Object | memcpy | memcpy |

Code Snippet

File Name freebsd-src-2/ips_commands.c

Method static void ips_drive_info_callback(void *cmdptr, bus_dma_segment_t *segments,int segnum, int error)

```
....
304.        memcpy(sc->drives, driveinfo->drives, sizeof(ips_drive_t) *
8);
```

## 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=1060098&projectid=60088&pathid=39 |
| Status | New |

The size of the buffer used by evbuffer_search_eol in it, at line 1590 of freebsd-src-2/buffer.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that evbuffer_search_eol passes to it, at line 1590 of freebsd-src-2/buffer.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1622 | 1622 |
| Object | it | it |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_search_eol(struct evbuffer *buffer,

```
....
1622.             memcpy(&it2, &it, sizeof(it));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=40 |
| Status | New |

The size of the buffer used by evbuffer_search_eol in it, at line 1590 of freebsd-src-2/buffer.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that evbuffer_search_eol passes to it, at line 1590 of freebsd-src-2/buffer.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1644 | 1644 |
| Object | it | it |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_search_eol(struct evbuffer *buffer,

```
....
1644.             memcpy(&it2, &it, sizeof(it));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=41 |
| Status | New |

The size of the buffer used by evbuffer_add_vprintf in va_list, at line 2831 of freebsd-src-2/buffer.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that evbuffer_add_vprintf passes to va_list, at line 2831 of freebsd-src-2/buffer.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |

| | | |
|---|---|---|
| Line | 2863 | 2863 |
| Object | va_list | va_list |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_add_vprintf(struct evbuffer *buf, const char *fmt, va_list ap)

```
....
2863.             va_copy(aq, ap);
```

**Buffer Overflow boundcpy WrongSizeParam\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=42 |
| Status | New |

The size of the buffer used by sendpacket in int, at line 85 of freebsd-src-2/cap_sendmsg.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sendpacket passes to int, at line 85 of freebsd-src-2/cap_sendmsg.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cap_sendmsg.c | freebsd-src-2/cap_sendmsg.c |
| Line | 120 | 120 |
| Object | int | int |

Code Snippet
File Name freebsd-src-2/cap_sendmsg.c
Method sendpacket(int sock, struct sockaddr_in6 *dst, uint32_t ifindex, int hoplimit,

```
....
120.        memcpy(CMSG_DATA(cm), &hoplimit, sizeof(int));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=43 |
| Status | New |

The size of the buffer used by *dtls1_get_timeout in timeval, at line 287 of freebsd-src-2/d1_lib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *dtls1_get_timeout passes to timeval, at line 287 of freebsd-src-2/d1_lib.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/d1_lib.c | freebsd-src-2/d1_lib.c |
| Line | 308 | 308 |

| | | |
|---|---|---|
| Object | timeval | timeval |

Code Snippet
File Name freebsd-src-2/d1_lib.c
Method struct timeval *dtls1_get_timeout(SSL *s, struct timeval *timeleft)

```
....
308.      memcpy(timeleft, &(s->d1->next_timeout), sizeof(struct
timeval));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=44
Status New

The size of the buffer used by mt7615_regd_notifier in Namespace1527133530, at line 331 of freebsd-src-2/init.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mt7615_regd_notifier passes to Namespace1527133530, at line 331 of freebsd-src-2/init.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/init.c | freebsd-src-2/init.c |
| Line | 340 | 340 |
| Object | Namespace1527133530 | Namespace1527133530 |

Code Snippet
File Name freebsd-src-2/init.c
Method mt7615_regd_notifier(struct wiphy *wiphy,

```
....
340.        memcpy(dev->mt76.alpha2, request->alpha2, sizeof(dev-
>mt76.alpha2));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 7:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=45
Status New

The size of the buffer used by dtls1_reset_seq_numbers in ->, at line 1037 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_reset_seq_numbers passes to ->, at line 1037 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |

| | | |
|---|---|---|
| Line | 1046 | 1046 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method void dtls1_reset_seq_numbers(SSL *s, int rw)

```
....
1046.                   sizeof(s->rlayer.d->bitmap));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=46 |
| Status | New |

The size of the buffer used by dtls1_reset_seq_numbers in Namespace1423434742, at line 1037 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_reset_seq_numbers passes to Namespace1423434742, at line 1037 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |
| Line | 1057 | 1057 |
| Object | Namespace1423434742 | Namespace1423434742 |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method void dtls1_reset_seq_numbers(SSL *s, int rw)

```
....
1057.                   sizeof(s->rlayer.write_sequence));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=47 |
| Status | New |

The size of the buffer used by DTLS_RECORD_LAYER_set_saved_w_epoch in ->, at line 101 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DTLS_RECORD_LAYER_set_saved_w_epoch passes to ->, at line 101 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |

| | | |
|---|---|---|
| Line | 105 | 105 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method void DTLS_RECORD_LAYER_set_saved_w_epoch(RECORD_LAYER *rl, unsigned short e)

```
....
105.                rl->write_sequence, sizeof(rl->write_sequence));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 10:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=48
Status New

The size of the buffer used by DTLS_RECORD_LAYER_set_saved_w_epoch in ->, at line 101 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DTLS_RECORD_LAYER_set_saved_w_epoch passes to ->, at line 101 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |
| Line | 107 | 107 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method void DTLS_RECORD_LAYER_set_saved_w_epoch(RECORD_LAYER *rl, unsigned short e)

```
....
107.                rl->d->last_write_sequence, sizeof(rl-
>write_sequence));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 11:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=49
Status New

The size of the buffer used by DTLS_RECORD_LAYER_set_saved_w_epoch in ->, at line 101 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DTLS_RECORD_LAYER_set_saved_w_epoch passes to ->, at line 101 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |
| Line | 112 | 112 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method void DTLS_RECORD_LAYER_set_saved_w_epoch(RECORD_LAYER *rl, unsigned short e)

```
....
112.                 rl->d->curr_write_sequence, sizeof(rl-
>write_sequence));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 12:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=50
Status New

The size of the buffer used by dtls1_copy_record in SSL3_BUFFER, at line 123 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_copy_record passes to SSL3_BUFFER, at line 123 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |
| Line | 133 | 133 |
| Object | SSL3_BUFFER | SSL3_BUFFER |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method static int dtls1_copy_record(SSL *s, pitem *item)

```
....
133.      memcpy(&s->rlayer.rbuf, &(rdata->rbuf), sizeof(SSL3_BUFFER));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 13:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=51
Status New

The size of the buffer used by dtls1_copy_record in SSL3_RECORD, at line 123 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that dtls1_copy_record passes to SSL3_RECORD, at line 123 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |
| Line | 134 | 134 |
| Object | SSL3_RECORD | SSL3_RECORD |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method static int dtls1_copy_record(SSL *s, pitem *item)

```
....
134.      memcpy(&s->rlayer.rrec, &(rdata->rrec), sizeof(SSL3_RECORD));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 14:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=52
Status New

The size of the buffer used by dtls1_buffer_record in SSL3_BUFFER, at line 142 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_buffer_record passes to SSL3_BUFFER, at line 142 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |
| Line | 163 | 163 |
| Object | SSL3_BUFFER | SSL3_BUFFER |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method int dtls1_buffer_record(SSL *s, record_pqueue *queue, unsigned char *priority)

```
....
163.      memcpy(&(rdata->rbuf), &s->rlayer.rbuf, sizeof(SSL3_BUFFER));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 15:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=53
Status New

The size of the buffer used by dtls1_buffer_record in SSL3_RECORD, at line 142 of freebsd-src-2/rec_layer_d1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that dtls1_buffer_record passes to SSL3_RECORD, at line 142 of freebsd-src-2/rec_layer_d1.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rec_layer_d1.c | freebsd-src-2/rec_layer_d1.c |
| Line | 164 | 164 |
| Object | SSL3_RECORD | SSL3_RECORD |

Code Snippet
File Name freebsd-src-2/rec_layer_d1.c
Method int dtls1_buffer_record(SSL *s, record_pqueue *queue, unsigned char *priority)

```
....
164.      memcpy(&(rdata->rrec), &s->rlayer.rrec, sizeof(SSL3_RECORD));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 16:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=54
Status New

The size of the buffer used by rdata2sockaddr in ->, at line 567 of freebsd-src-2/respip.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rdata2sockaddr passes to ->, at line 567 of freebsd-src-2/respip.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 578 | 578 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/respip.c
Method rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i,

```
....
578.                    sizeof(sa4->sin_addr));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 17:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=55
Status New

The size of the buffer used by rdata2sockaddr in ->, at line 567 of freebsd-src-2/respip.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rdata2sockaddr passes to ->, at line 567 of freebsd-src-2/respip.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 587 | 587 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/respip.c
Method rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i,

```
....
587.                    sizeof(sa6->sin6_addr));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 18:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=56
Status New

The size of the buffer used by rtsol_input in Namespace1278039934, at line 159 of freebsd-src-2/rtsol.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rtsol_input passes to Namespace1278039934, at line 159 of freebsd-src-2/rtsol.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 352 | 352 |
| Object | Namespace1278039934 | Namespace1278039934 |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
352.                  sizeof(rai->rai_saddr.sin6_addr));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 19:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=57
Status New

The size of the buffer used by session_setup_x11fwd in in_addr, at line 2589 of freebsd-src-2/session.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session_setup_x11fwd passes to in_addr, at line 2589 of freebsd-src-2/session.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 2650 | 2650 |
| Object | in_addr | in_addr |

Code Snippet
File Name freebsd-src-2/session.c
Method session_setup_x11fwd(struct ssh *ssh, Session *s)

```
....
2650.             memcpy(&my_addr, he->h_addr_list[0], sizeof(struct
in_addr));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 20:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=58
Status New

The size of the buffer used by dtls1_reassemble_fragment in msg_hdr, at line 531 of freebsd-src-2/statem_dtls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_reassemble_fragment passes to msg_hdr, at line 531 of freebsd-src-2/statem_dtls.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 558 | 558 |
| Object | msg_hdr | msg_hdr |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr)

```
....
558.          memcpy(&(frag->msg_header), msg_hdr, sizeof(*msg_hdr));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 21:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=59
Status New

The size of the buffer used by dtls1_process_out_of_seq_message in msg_hdr, at line 640 of freebsd-src-2/statem_dtls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_process_out_of_seq_message passes to msg_hdr, at line 640 of freebsd-src-2/statem_dtls.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 697 | 697 |
| Object | msg_hdr | msg_hdr |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_process_out_of_seq_message(SSL *s, const struct hm_header_st *msg_hdr)

```
....
697.          memcpy(&(frag->msg_header), msg_hdr, sizeof(*msg_hdr));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 22:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=60
Status New

The size of the buffer used by ossl_statem_server_post_work in DTLS1_SCTP_AUTH_LABEL, at line 808 of freebsd-src-2/statem_srvr.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ossl_statem_server_post_work passes to DTLS1_SCTP_AUTH_LABEL, at line 808 of freebsd-src-2/statem_srvr.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 861 | 861 |
| Object | DTLS1_SCTP_AUTH_LABEL | DTLS1_SCTP_AUTH_LABEL |

Code Snippet
File Name freebsd-src-2/statem_srvr.c
Method WORK_STATE ossl_statem_server_post_work(SSL *s, WORK_STATE wst)

```
....
861.                      sizeof(DTLS1_SCTP_AUTH_LABEL));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 23:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=61
Status New

The size of the buffer used by tls_post_process_client_key_exchange in DTLS1_SCTP_AUTH_LABEL, at line 3525 of freebsd-src-2/statem_srvr.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls_post_process_client_key_exchange passes to DTLS1_SCTP_AUTH_LABEL, at line 3525 of freebsd-src-2/statem_srvr.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 3538 | 3538 |
| Object | DTLS1_SCTP_AUTH_LABEL | DTLS1_SCTP_AUTH_LABEL |

Code Snippet
File Name freebsd-src-2/statem_srvr.c
Method WORK_STATE tls_post_process_client_key_exchange(SSL *s, WORK_STATE wst)

```
....
3538.                       sizeof(DTLS1_SCTP_AUTH_LABEL));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 24:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=62
Status New

The size of the buffer used by construct_stateless_ticket in Namespace1690719778, at line 3865 of freebsd-src-2/statem_srvr.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that construct_stateless_ticket passes to Namespace1690719778, at line 3865 of freebsd-src-2/statem_srvr.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 3988 | 3988 |
| Object | Namespace1690719778 | Namespace1690719778 |

Code Snippet
File Name freebsd-src-2/statem_srvr.c
Method static int construct_stateless_ticket(SSL *s, WPACKET *pkt, uint32_t age_add,

```
....
3988.                   sizeof(tctx->ext.tick_key_name));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 25:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=63
Status New

The size of the buffer used by fcntl_getlock_pids in lock, at line 854 of freebsd-src-2/t_vnops.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fcntl_getlock_pids passes to lock, at line 854 of freebsd-src-2/t_vnops.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 878 | 878 |
| Object | lock | lock |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method fcntl_getlock_pids(const atf_tc_t *tc, const char *mp)

```
....
878.        memcpy(expect, lock, sizeof(lock));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=64 |
| Status | New |

The size of the buffer used by tcp_set_cc_mod in cc_var, at line 1925 of freebsd-src-2/tcp_usrreq.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tcp_set_cc_mod passes to cc_var, at line 1925 of freebsd-src-2/tcp_usrreq.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tcp_usrreq.c | freebsd-src-2/tcp_usrreq.c |
| Line | 2019 | 2019 |
| Object | cc_var | cc_var |

Code Snippet
File Name freebsd-src-2/tcp_usrreq.c
Method tcp_set_cc_mod(struct inpcb *inp, struct sockopt *sopt)

```
....
2019.            memcpy(&tp->t_ccv, &cc_mem, sizeof(struct cc_var));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=65 |
| Status | New |

The size of the buffer used by wlan_get_local_addr in sockaddr_dl, at line 286 of freebsd-src-2/wlan_sys.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that wlan_get_local_addr passes to sockaddr_dl, at line 286 of freebsd-src-2/wlan_sys.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 302 | 302 |
| Object | sockaddr_dl | sockaddr_dl |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_local_addr(struct wlan_iface *wif)

```
....
302.              memcpy(&sdl, ifa->ifa_addr, sizeof(struct
sockaddr_dl));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=66 |
| Status | New |

The size of the buffer used by wlan_get_channel_list in c, at line 587 of freebsd-src-2/wlan_sys.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that wlan_get_channel_list passes to c, at line 587 of freebsd-src-2/wlan_sys.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 626 | 626 |
| Object | c | c |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_channel_list(struct wlan_iface *wif)

```
....
626.              memcpy(wif->chanlist + nchans, c, sizeof (*c));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=67 |
| Status | New |

The size of the buffer used by wlan_get_scan_results in ieee80211req_scan_result, at line 2187 of freebsd-src-2/wlan_sys.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that wlan_get_scan_results passes to ieee80211req_scan_result, at line 2187 of freebsd-src-2/wlan_sys.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 2206 | 2206 |
| Object | ieee80211req_scan_result | ieee80211req_scan_result |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_scan_results(struct wlan_iface *wif)

```
....
2206.             memcpy(&isr, cp, sizeof(struct
ieee80211req_scan_result));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=68 |
| Status | New |

The size of the buffer used by wlan_get_peerinfo in ieee80211req_sta_info, at line 2714 of freebsd-src-2/wlan_sys.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that wlan_get_peerinfo passes to ieee80211req_sta_info, at line 2714 of freebsd-src-2/wlan_sys.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 2739 | 2739 |
| Object | ieee80211req_sta_info | ieee80211req_sta_info |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_peerinfo(struct wlan_iface *wif)

```
....
2739.             memcpy(&si, cp, sizeof(struct ieee80211req_sta_info));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=69 |
| Status | New |

The size of the buffer used by wlan_mesh_get_routelist in rt, at line 3036 of freebsd-src-2/wlan_sys.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that wlan_mesh_get_routelist passes to rt, at line 3036 of freebsd-src-2/wlan_sys.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 3054 | 3054 |
| Object | rt | rt |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_mesh_get_routelist(struct wlan_iface *wif)

```
....
3054.             memcpy(&wmr->imroute, rt, sizeof(*rt));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=70 |
| Status | New |

The size of the buffer used by X86_64::writePltHeader in pltData, at line 396 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that X86_64::writePltHeader passes to pltData, at line 396 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 402 | 402 |
| Object | pltData | pltData |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void X86_64::writePltHeader(uint8_t *buf) const {

```
....
402.    memcpy(buf, pltData, sizeof(pltData));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=71 |
| Status | New |

The size of the buffer used by X86_64::writePlt in inst, at line 409 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that X86_64::writePlt passes to inst, at line 409 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 416 | 416 |
| Object | inst | inst |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void X86_64::writePlt(uint8_t *buf, const Symbol &sym,

```
....
416.    memcpy(buf, inst, sizeof(inst));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=72 |
| Status | New |

The size of the buffer used by X86_64::relaxTlsGdToLe in inst, at line 430 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that X86_64::relaxTlsGdToLe passes to inst, at line 430 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 445 | 445 |
| Object | inst | inst |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void X86_64::relaxTlsGdToLe(uint8_t *loc, const Relocation &rel,

```
....
445.      memcpy(loc - 4, inst, sizeof(inst));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=73 |
| Status | New |

The size of the buffer used by X86_64::relaxTlsGdToIe in inst, at line 471 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that X86_64::relaxTlsGdToIe passes to inst, at line 471 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 486 | 486 |
| Object | inst | inst |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void X86_64::relaxTlsGdToIe(uint8_t *loc, const Relocation &rel,

```
....
486.      memcpy(loc - 4, inst, sizeof(inst));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=74 |
| Status | New |

The size of the buffer used by X86_64::relaxTlsLdToLe in inst, at line 555 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that X86_64::relaxTlsLdToLe passes to inst, at line 555 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 582 | 582 |
| Object | inst | inst |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void X86_64::relaxTlsLdToLe(uint8_t *loc, const Relocation &rel,

```
....
582.      memcpy(loc - 3, inst, sizeof(inst));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=75 |
| Status | New |

The size of the buffer used by X86_64::relaxTlsLdToLe in inst, at line 555 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that X86_64::relaxTlsLdToLe passes to inst, at line 555 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 596 | 596 |
| Object | inst | inst |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void X86_64::relaxTlsLdToLe(uint8_t *loc, const Relocation &rel,

```
....
596.      memcpy(loc - 2, inst, sizeof(inst));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=76 |
| Status | New |

The size of the buffer used by IntelIBT::writeIBTPlt in inst, at line 1012 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IntelIBT::writeIBTPlt passes to inst, at line 1012 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 1024 | 1024 |
| Object | inst | inst |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void IntelIBT::writeIBTPlt(uint8_t *buf, size_t numEntries) const {

```
....
1024.      memcpy(buf, inst, sizeof(inst));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=77 |
| Status | New |

The size of the buffer used by IntelIBT::writePlt in Inst, at line 1001 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IntelIBT::writePlt passes to Inst, at line 1001 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 1008 | 1008 |
| Object | Inst | Inst |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void IntelIBT::writePlt(uint8_t *buf, const Symbol &sym,

```
....
1008.    memcpy(buf, Inst, sizeof(Inst));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=78 |
| Status | New |

The size of the buffer used by Retpoline::writePlt in insn, at line 1092 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Retpoline::writePlt passes to insn, at line 1092 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 1102 | 1102 |
| Object | insn | insn |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void Retpoline::writePlt(uint8_t *buf, const Symbol &sym,

```
....
1102.    memcpy(buf, insn, sizeof(insn));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=79 |
| Status | New |

The size of the buffer used by Retpoline::writePltHeader in insn, at line 1070 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Retpoline::writePltHeader passes to insn, at line 1070 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 1084 | 1084 |
| Object | insn | insn |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void Retpoline::writePltHeader(uint8_t *buf) const {

```
....
1084.    memcpy(buf, insn, sizeof(insn));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=80 |
| Status | New |

The size of the buffer used by RetpolineZNow::writePlt in insn, at line 1135 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RetpolineZNow::writePlt passes to insn, at line 1135 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 1142 | 1142 |
| Object | insn | insn |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void RetpolineZNow::writePlt(uint8_t *buf, const Symbol &sym,

```
....
1142.    memcpy(buf, insn, sizeof(insn));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=81 |
| Status | New |

The size of the buffer used by RetpolineZNow::writePltHeader in insn, at line 1119 of freebsd-src-2/X86_64.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that RetpolineZNow::writePltHeader passes to insn, at line 1119 of freebsd-src-2/X86_64.cpp, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 1132 | 1132 |
| Object | insn | insn |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method void RetpolineZNow::writePltHeader(uint8_t *buf) const {

```
....
1132.    memcpy(buf, insn, sizeof(insn));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=82 |
| Status | New |

The size of the buffer used by ext4_ext_grow_indepth in ->, at line 1084 of freebsd-src-2/ext2_extents.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ext4_ext_grow_indepth passes to ->, at line 1084 of freebsd-src-2/ext2_extents.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1108 | 1108 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_grow_indepth(struct inode *ip, struct ext4_extent_path *path,

```
....
1108.        memmove(bp->b_data, curpath->ep_header, sizeof(ip->i_data));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=83 |
| Status | New |

The size of the buffer used by sendpacket in ->, at line 85 of freebsd-src-2/cap_sendmsg.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sendpacket passes to ->, at line 85 of freebsd-src-2/cap_sendmsg.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cap_sendmsg.c | freebsd-src-2/cap_sendmsg.c |

| | | |
|---|---|---|
| Line | 112 | 112 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/cap_sendmsg.c
Method sendpacket(int sock, struct sockaddr_in6 *dst, uint32_t ifindex, int hoplimit,

```
....
112.        memset(&pi->ipi6_addr, 0, sizeof(pi->ipi6_addr));
      /*XXX*/
```

**Buffer Overflow boundcpy WrongSizeParam\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=84 |
| Status | New |

The size of the buffer used by dtls1_clear in s, at line 155 of freebsd-src-2/d1_lib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_clear passes to s, at line 155 of freebsd-src-2/d1_lib.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/d1_lib.c | freebsd-src-2/d1_lib.c |
| Line | 174 | 174 |
| Object | s | s |

Code Snippet
File Name freebsd-src-2/d1_lib.c
Method int dtls1_clear(SSL *s)

```
....
174.          memset(s->d1, 0, sizeof(*s->d1));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=85 |
| Status | New |

The size of the buffer used by dtls1_start_timer in ->, at line 243 of freebsd-src-2/d1_lib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_start_timer passes to ->, at line 243 of freebsd-src-2/d1_lib.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/d1_lib.c | freebsd-src-2/d1_lib.c |
| Line | 250 | 250 |

| | | |
|---|---|---|
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/d1_lib.c
Method void dtls1_start_timer(SSL *s)

```
....
250.          memset(&s->d1->next_timeout, 0, sizeof(s->d1-
>next_timeout));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=86 |
| Status | New |

The size of the buffer used by dtls1_stop_timer in ->, at line 352 of freebsd-src-2/d1_lib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_stop_timer passes to ->, at line 352 of freebsd-src-2/d1_lib.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/d1_lib.c | freebsd-src-2/d1_lib.c |
| Line | 355 | 355 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/d1_lib.c
Method void dtls1_stop_timer(SSL *s)

```
....
355.      memset(&s->d1->timeout, 0, sizeof(s->d1->timeout));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=87 |
| Status | New |

The size of the buffer used by dtls1_stop_timer in ->, at line 352 of freebsd-src-2/d1_lib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_stop_timer passes to ->, at line 352 of freebsd-src-2/d1_lib.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/d1_lib.c | freebsd-src-2/d1_lib.c |
| Line | 356 | 356 |
| Object | -> | -> |

Code Snippet
File Name freebsd-src-2/d1_lib.c
Method void dtls1_stop_timer(SSL *s)

```
....
356.      memset(&s->d1->next_timeout, 0, sizeof(s->d1->next_timeout));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=88 |
| Status | New |

The size of the buffer used by main in stat, at line 129 of freebsd-src-2/diff.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 stat, at line 129 of freebsd-src-2/diff.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/diff.c | freebsd-src-2/diff.c |
| Line | 402 | 402 |
| Object | stat | stat |

Code Snippet
File Name freebsd-src-2/diff.c
Method main(int argc, char **argv)

```
....
402.              memset(&stb1, 0, sizeof(struct stat));
```

## 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=1060098&projectid=60088&pathid=213 |
| Status | New |

Calling free() (line 965) on a variable that was not dynamically allocated (line 965) in file freebsd-src-2/acpi_thermal.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/acpi_thermal.c | freebsd-src-2/acpi_thermal.c |
| Line | 984 | 984 |

| | | |
|---|---|---|
| Object | devs | devs |

Code Snippet
File Name freebsd-src-2/acpi_thermal.c
Method acpi_tz_thread(void *arg)

```
....
984.                free(devs, M_TEMP);
```

**MemoryFree on StackVariable\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=214 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 149 | 149 |
| Object | nm | nm |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
149.                free(nm);
```

**MemoryFree on StackVariable\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=215 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 150 | 150 |
| Object | tp | tp |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/cachedump.c |
| Method | dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k) |

```
....
150.                free(tp);
```

**MemoryFree on StackVariable\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=216 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 151 | 151 |
| Object | cl | cl |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/cachedump.c |
| Method | dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k) |

```
....
151.                free(cl);
```

**MemoryFree on StackVariable\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=217 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 155 | 155 |
| Object | nm | nm |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/cachedump.c |
| Method | dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k) |

```
....
155.                free(nm);
```

**MemoryFree on StackVariable\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=218 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 156 | 156 |
| Object | tp | tp |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
156.                free(tp);
```

**MemoryFree on StackVariable\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=219 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 157 | 157 |
| Object | cl | cl |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
157.                free(cl);
```

**MemoryFree on StackVariable\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=220 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 160 | 160 |
| Object | nm | nm |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
160.          free(nm);
```

**MemoryFree on StackVariable\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=221 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 161 | 161 |
| Object | tp | tp |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
161.        free(tp);
```

**MemoryFree on StackVariable\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=222 |
| Status | New |

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 162 | 162 |
| Object | cl | cl |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
162.        free(cl);
```

**MemoryFree on StackVariable\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=223 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 181 | 181 |
| Object | nm | nm |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
181.                free(nm);
```

**MemoryFree on StackVariable\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=224 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 182 | 182 |
| Object | tp | tp |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
182.                free(tp);
```

**MemoryFree on StackVariable\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=225 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 183 | 183 |
| Object | cl | cl |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
183.                free(cl);
```

**MemoryFree on StackVariable\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=226 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 188 | 188 |
| Object | nm | nm |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
188.                free(nm);
```

**MemoryFree on StackVariable\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=227 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 189 | 189 |
| Object | tp | tp |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
189.                free(tp);
```

**MemoryFree on StackVariable\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=228 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 190 | 190 |
| Object | cl | cl |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
190.                free(cl);
```

**MemoryFree on StackVariable\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=229 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 202 | 202 |
| Object | nm | nm |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
202.                free(nm);
```

**MemoryFree on StackVariable\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=230 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 203 | 203 |
| Object | tp | tp |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
203.                free(tp);
```

**MemoryFree on StackVariable\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=231 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 204 | 204 |
| Object | cl | cl |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
204.                free(cl);
```

**MemoryFree on StackVariable\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=232 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 208 | 208 |
| Object | nm | nm |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
208.          free(nm);
```

**MemoryFree on StackVariable\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=233 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 209 | 209 |
| Object | tp | tp |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
209.        free(tp);
```

**MemoryFree on StackVariable\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=234 |
| Status | New |

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file freebsd-src-2/cachedump.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 210 | 210 |
| Object | cl | cl |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
210.        free(cl);
```

**MemoryFree on StackVariable\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=235 |
| Status | New |

Calling free() (line 123) on a variable that was not dynamically allocated (line 123) in file freebsd-src-2/dtstream.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 129 | 129 |
| Object | e | e |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method dt_msg_queue_clear(struct dt_msg_queue* mq)

```
....
129.                free(e);
```

**MemoryFree on StackVariable\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=236 |
| Status | New |

Calling free() (line 307) on a variable that was not dynamically allocated (line 307) in file freebsd-src-2/dtstream.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 315 | 315 |
| Object | item | item |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method void dt_io_thread_delete(struct dt_io_thread* dtio)

```
....
315.                free(item);
```

**MemoryFree on StackVariable\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=237 |
| Status | New |

Calling free() (line 463) on a variable that was not dynamically allocated (line 463) in file freebsd-src-2/dtstream.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 478 | 478 |
| Object | item | item |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method void dt_io_thread_unregister_queue(struct dt_io_thread* dtio,

```
....
478.                    free(item);
```

**MemoryFree on StackVariable\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=238 |
| Status | New |

Calling free() (line 489) on a variable that was not dynamically allocated (line 489) in file freebsd-src-2/dtstream.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 503 | 503 |
| Object | entry | entry |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method static int dt_msg_queue_pop(struct dt_msg_queue* mq, void** buf,

```
....
503.                free(entry);
```

**MemoryFree on StackVariable\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=239 |
| Status | New |

Calling free() (line 159) on a variable that was not dynamically allocated (line 159) in file freebsd-src-2/http-server.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 316 | 316 |
| Object | decoded_path | decoded_path |

Code Snippet
File Name freebsd-src-2/http-server.c
Method send_document_cb(struct evhttp_request *req, void *arg)

```
....
316.              free(decoded_path);
```

**MemoryFree on StackVariable\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=240 |
| Status | New |

Calling free() (line 455) on a variable that was not dynamically allocated (line 455) in file freebsd-src-2/mem_dbg.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/mem_dbg.c | freebsd-src-2/mem_dbg.c |
| Line | 562 | 562 |
| Object | strings | strings |

Code Snippet
File Name freebsd-src-2/mem_dbg.c
Method static void print_leak(const MEM *m, MEM_LEAK *l)

```
....
562.          free(strings);
```

**MemoryFree on StackVariable\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=241 |
| Status | New |

Calling free() (line 73) on a variable that was not dynamically allocated (line 73) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 93 | 93 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_name(krb5_context context,

```
....
93.    free(name);
```

**MemoryFree on StackVariable\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=242 |
| Status | New |

Calling free() (line 73) on a variable that was not dynamically allocated (line 73) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 100 | 100 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_name(krb5_context context,

```
....
100.         free(name);
```

**MemoryFree on StackVariable\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=243 |
| Status | New |

Calling free() (line 73) on a variable that was not dynamically allocated (line 73) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 104 | 104 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_name(krb5_context context,

```
....
104.        free(name);
```

**MemoryFree on StackVariable\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=244 |
| Status | New |

Calling free() (line 116) on a variable that was not dynamically allocated (line 116) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 133 | 133 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_gen_new(krb5_context context,

```
....
133.        free(name);
```

**MemoryFree on StackVariable\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=245 |
| Status | New |

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 169 | 169 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_initialize(krb5_context context,

```
....
169.        free(name);
```

**MemoryFree on StackVariable\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=246 |
| Status | New |

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 175 | 175 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_initialize(krb5_context context,

```
....
175.        free(name);
```

**MemoryFree on StackVariable\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=247 |
| Status | New |

Calling free() (line 147) on a variable that was not dynamically allocated (line 147) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 182 | 182 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_initialize(krb5_context context,

```
....
182.        free(name);
```

**MemoryFree on StackVariable\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=248 |
| Status | New |

Calling free() (line 213) on a variable that was not dynamically allocated (line 213) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 232 | 232 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_destroy(krb5_context context,

```
....
232.        free(name);
```

**MemoryFree on StackVariable\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=249 |
| Status | New |

Calling free() (line 246) on a variable that was not dynamically allocated (line 246) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 265 | 265 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_store(krb5_context context,

```
....
265.        free(name);
```

**MemoryFree on StackVariable\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=250 |
| Status | New |

Calling free() (line 246) on a variable that was not dynamically allocated (line 246) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 272 | 272 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_store(krb5_context context,

```
....
272.        free(name);
```

**MemoryFree on StackVariable\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=251 |
| Status | New |

Calling free() (line 246) on a variable that was not dynamically allocated (line 246) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 279 | 279 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_store(krb5_context context,

```
....
279.        free(name);
```

**MemoryFree on StackVariable\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=252 |
| Status | New |

Calling free() (line 246) on a variable that was not dynamically allocated (line 246) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 287 | 287 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_store(krb5_context context,

```
....
287.        free(name);
```

**MemoryFree on StackVariable\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=253 |
| Status | New |

Calling free() (line 304) on a variable that was not dynamically allocated (line 304) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 326 | 326 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_retrieve(krb5_context context,

```
....
326.        free(name);
```

**MemoryFree on StackVariable\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=254 |
| Status | New |

Calling free() (line 304) on a variable that was not dynamically allocated (line 304) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 332 | 332 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_retrieve(krb5_context context,

```
....
332.        free(name);
```

**MemoryFree on StackVariable\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=255 |
| Status | New |

Calling free() (line 304) on a variable that was not dynamically allocated (line 304) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 340 | 340 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_retrieve(krb5_context context,

```
....
340.         free(name);
```

**MemoryFree on StackVariable\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=256 |
| Status | New |

Calling free() (line 304) on a variable that was not dynamically allocated (line 304) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 348 | 348 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_retrieve(krb5_context context,

```
....
348.         free(name);
```

**MemoryFree on StackVariable\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=257 |
| Status | New |

Calling free() (line 304) on a variable that was not dynamically allocated (line 304) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 377 | 377 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_retrieve(krb5_context context,

```
....
377.        free(name);
```

**MemoryFree on StackVariable\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=258 |
| Status | New |

Calling free() (line 395) on a variable that was not dynamically allocated (line 395) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 414 | 414 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_principal(krb5_context context,

```
....
414.        free(name);
```

**MemoryFree on StackVariable\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=259 |
| Status | New |

Calling free() (line 395) on a variable that was not dynamically allocated (line 395) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 423 | 423 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_principal(krb5_context context,

```
....
423.        free(name);
```

**MemoryFree on StackVariable\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=260 |
| Status | New |

Calling free() (line 438) on a variable that was not dynamically allocated (line 438) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 457 | 457 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_cred_uuid_list(krb5_context context,

```
....
457.        free(name);
```

**MemoryFree on StackVariable\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=261 |
| Status | New |

Calling free() (line 484) on a variable that was not dynamically allocated (line 484) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 505 | 505 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_cred_by_uuid(krb5_context context,

```
....
505.        free(name);
```

**MemoryFree on StackVariable\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=262 |
| Status | New |

Calling free() (line 541) on a variable that was not dynamically allocated (line 541) in file freebsd-src-2/protocol.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 561 | 561 |
| Object | name | name |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_remove_cred(krb5_context context,

```
....
561.        free(name);
```

## 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=1060098&projectid=60088&pathid=856 |
| Status | New |

The variable declared in ecdh at freebsd-src-2/crypto_wolfssl.c in line 1699 is not initialized when it is used by ecdh at freebsd-src-2/crypto_wolfssl.c in line 1699.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/crypto_wolfssl.c | freebsd-src-2/crypto_wolfssl.c |
| Line | 1701 | 1708 |

| | | |
|---|---|---|
| Object | ecdh | ecdh |

Code Snippet
File Name freebsd-src-2/crypto_wolfssl.c
Method struct crypto_ecdh * crypto_ecdh_init(int group)

```
....
1701.       struct crypto_ecdh *ecdh = NULL;
....
1708.       ecdh = os_zalloc(sizeof(*ecdh));
```

**Use of Zero Initialized Pointer\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=857
Status New

The variable declared in additional at freebsd-src-2/drbg_lib.c in line 646 is not initialized when it is used by adin at freebsd-src-2/drbg_lib.c in line 566.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/drbg_lib.c | freebsd-src-2/drbg_lib.c |
| Line | 648 | 568 |
| Object | additional | adin |

Code Snippet
File Name freebsd-src-2/drbg_lib.c
Method int RAND_DRBG_bytes(RAND_DRBG *drbg, unsigned char *out, size_t outlen)

```
....
648.      unsigned char *additional = NULL;
```

File Name freebsd-src-2/drbg_lib.c
Method int RAND_DRBG_generate(RAND_DRBG *drbg, unsigned char *out, size_t outlen,

```
....
568.                           const unsigned char *adin, size_t adinlen)
```

**Use of Zero Initialized Pointer\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=858
Status New

The variable declared in qp at freebsd-src-2/fbsd_kcompat.c in line 773 is not initialized when it is used by qp at freebsd-src-2/fbsd_kcompat.c in line 773.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/fbsd_kcompat.c | freebsd-src-2/fbsd_kcompat.c |
| Line | 775 | 781 |
| Object | qp | qp |

Code Snippet
File Name freebsd-src-2/fbsd_kcompat.c
Method irdma_cleanup_dead_qps(struct irdma_sc_vsi *vsi)

```
....
775.        struct irdma_sc_qp *qp = NULL;
....
781.                qp = irdma_get_qp_from_list(&vsi->qos[i].qplist, qp);
```

**Use of Zero Initialized Pointer\Path 4:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=859
Status New

The variable declared in cm at freebsd-src-2/ip6_output.c in line 2800 is not initialized when it is used by cm at freebsd-src-2/ip6_output.c in line 2800.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2803 | 2852 |
| Object | cm | cm |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopts(struct mbuf *control, struct ip6_pktopts *opt,

```
....
2803.       struct cmsghdr *cm = NULL;
....
2852.                   cm->cmsg_len - CMSG_LEN(0), opt, cred, 0, 1,
uproto);
```

**Use of Zero Initialized Pointer\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=860
Status New

The variable declared in cm at freebsd-src-2/ip6_output.c in line 2800 is not initialized when it is used by cm at freebsd-src-2/ip6_output.c in line 2800.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2803 | 2851 |
| Object | cm | cm |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopts(struct mbuf *control, struct ip6_pktopts *opt,

```
....
2803.        struct cmsghdr *cm = NULL;
....
2851.                error = ip6_setpktopt(cm->cmsg_type, CMSG_DATA(cm),
```

**Use of Zero Initialized Pointer\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=861
Status New

The variable declared in server at freebsd-src-2/protocol.c in line 754 is not initialized when it is used by server at freebsd-src-2/protocol.c in line 754.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 764 | 809 |
| Object | server | server |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_get_initial_ticket(krb5_context context,

```
....
764.      krb5_principal server = NULL;
....
809.        ccache->server = server;
```

**Use of Zero Initialized Pointer\Path 7:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=862
Status New

The variable declared in pi at freebsd-src-2/rtsol.c in line 159 is not initialized when it is used by pi at freebsd-src-2/rtsol.c in line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 169 | 245 |
| Object | pi | pi |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
169.        struct in6_pktinfo *pi = NULL;
....
245.                    if_indextoname(pi->ipi6_ifindex, ifnamebuf));
```

**Use of Zero Initialized Pointer\Path 8:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=863
Status New

The variable declared in pi at freebsd-src-2/rtsol.c in line 159 is not initialized when it is used by pi at freebsd-src-2/rtsol.c in line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 169 | 254 |
| Object | pi | pi |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
169.        struct in6_pktinfo *pi = NULL;
....
254.                    if_indextoname(pi->ipi6_ifindex, ifnamebuf));
```

**Use of Zero Initialized Pointer\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=864
Status New

The variable declared in pi at freebsd-src-2/rtsol.c in line 159 is not initialized when it is used by pi at freebsd-src-2/rtsol.c in line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 169 | 264 |
| Object | pi | pi |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
169.        struct in6_pktinfo *pi = NULL;
....
264.                    if_indextoname(pi->ipi6_ifindex, ifnamebuf));
```

**Use of Zero Initialized Pointer\Path 10:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=865
Status New

The variable declared in patterns at freebsd-src-2/scp.c in line 1648 is not initialized when it is used by patterns at freebsd-src-2/scp.c in line 1648.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1661 | 1957 |
| Object | patterns | patterns |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1661.       char **patterns = NULL;
....
1957.             free(patterns[n]);
```

**Use of Zero Initialized Pointer\Path 11:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=866
Status New

The variable declared in Pointer at freebsd-src-2/scp.c in line 946 is not initialized when it is used by patterns at freebsd-src-2/scp.c in line 1648.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 952 | 1957 |
| Object | Pointer | patterns |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
952.         *patternsp = NULL;
```

File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1957.             free(patterns[n]);
```

**Use of Zero Initialized Pointer\Path 12:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=867
Status New

The variable declared in done at freebsd-src-2/scp.c in line 946 is not initialized when it is used by patterns at freebsd-src-2/scp.c in line 1648.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 997 | 1957 |
| Object | done | patterns |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
997.         done = NULL;
```

File Name freebsd-src-2/scp.c

| | |
|---|---|
| Method | sink(int argc, char **argv, const char *src) |

```
....
1957.              free(patterns[n]);
```

**Use of Zero Initialized Pointer\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=868 |
| Status | New |

The variable declared in cmd at freebsd-src-2/session.c in line 1218 is not initialized when it is used by f at freebsd-src-2/session.c in line 1218.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1221 | 1238 |
| Object | cmd | f |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/session.c |
| Method | do_rc_files(struct ssh *ssh, Session *s, const char *shell) |

```
....
1221.        char *cmd = NULL, *user_rc = NULL;
....
1238.              f = popen(cmd, "w");
```

**Use of Zero Initialized Pointer\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=869 |
| Status | New |

The variable declared in cmd at freebsd-src-2/session.c in line 1218 is not initialized when it is used by f at freebsd-src-2/session.c in line 1218.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1221 | 1273 |
| Object | cmd | f |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/session.c |
| Method | do_rc_files(struct ssh *ssh, Session *s, const char *shell) |

```
....
1221.       char *cmd = NULL, *user_rc = NULL;
....
1273.             f = popen(cmd, "w");
```

**Use of Zero Initialized Pointer\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=870 |
| Status | New |

The variable declared in buf at freebsd-src-2/statem_dtls.c in line 56 is not initialized when it is used by frag at freebsd-src-2/statem_dtls.c in line 56.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 59 | 76 |
| Object | buf | frag |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method static hm_fragment *dtls1_hm_fragment_new(size_t frag_len, int reassembly)

```
....
59.      unsigned char *buf = NULL;
....
76.      frag->fragment = buf;
```

**Use of Zero Initialized Pointer\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=871 |
| Status | New |

The variable declared in frag at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by reassembly at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 565 | 600 |
| Object | frag | reassembly |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr)

```
....
565.                frag = NULL;
....
600.      RSMBLY_BITMASK_MARK(frag->reassembly, (long)msg_hdr->frag_off,
```

**Use of Zero Initialized Pointer\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=872 |
| Status | New |

The variable declared in reassembly at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by frag at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 610 | 609 |
| Object | reassembly | frag |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr)

```
....
610.          frag->reassembly = NULL;
....
609.          OPENSSL_free(frag->reassembly);
```

**Use of Zero Initialized Pointer\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=873 |
| Status | New |

The variable declared in frag at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by frag at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 565 | 609 |
| Object | frag | frag |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr)

```
....
565.              frag = NULL;
....
609.          OPENSSL_free(frag->reassembly);
```

**Use of Zero Initialized Pointer\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=874 |
| Status | New |

The variable declared in frag at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by reassembly at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 565 | 600 |
| Object | frag | reassembly |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr)

```
....
565.              frag = NULL;
....
600.      RSMBLY_BITMASK_MARK(frag->reassembly, (long)msg_hdr->frag_off,
```

**Use of Zero Initialized Pointer\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=875 |
| Status | New |

The variable declared in frag at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by reassembly at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 565 | 600 |
| Object | frag | reassembly |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr)

```
....
565.              frag = NULL;
....
600.      RSMBLY_BITMASK_MARK(frag->reassembly, (long)msg_hdr->frag_off,
```

**Use of Zero Initialized Pointer\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=876 |
| Status | New |

The variable declared in frag at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by frag at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 565 | 593 |
| Object | frag | frag |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr)

```
....
565.              frag = NULL;
....
593.                                      frag->fragment + msg_hdr-
>frag_off,
```

**Use of Zero Initialized Pointer\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=877 |
| Status | New |

The variable declared in bitmask at freebsd-src-2/statem_dtls.c in line 56 is not initialized when it is used by reassembly at freebsd-src-2/statem_dtls.c in line 56.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 60 | 89 |
| Object | bitmask | reassembly |

Code Snippet
File Name freebsd-src-2/statem_dtls.c

| | |
|---|---|
| Method | static hm_fragment *dtls1_hm_fragment_new(size_t frag_len, int reassembly) |

```
....
60.      unsigned char *bitmask = NULL;
....
89.      frag->reassembly = bitmask;
```

**Use of Zero Initialized Pointer\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=878 |
| Status | New |

The variable declared in clienthello at freebsd-src-2/statem_srvr.c in line 1383 is not initialized when it is used by clienthello at freebsd-src-2/statem_srvr.c in line 1383.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 1388 | 1408 |
| Object | clienthello | clienthello |

Code Snippet
File Name freebsd-src-2/statem_srvr.c
Method MSG_PROCESS_RETURN tls_process_client_hello(SSL *s, PACKET *pkt)

```
....
1388.      CLIENTHELLO_MSG *clienthello = NULL;
....
1408.      clienthello = OPENSSL_zalloc(sizeof(*clienthello));
```

**Use of Zero Initialized Pointer\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=879 |
| Status | New |

The variable declared in comp at freebsd-src-2/statem_srvr.c in line 1611 is not initialized when it is used by new_compression at freebsd-src-2/statem_srvr.c in line 1611.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 1619 | 2051 |
| Object | comp | new_compression |

Code Snippet
File Name freebsd-src-2/statem_srvr.c

Method static int tls_early_post_process_client_hello(SSL *s)

```
....
1619.      SSL_COMP *comp = NULL;
....
2051.              s->s3->tmp.new_compression = comp;
```

**Use of Zero Initialized Pointer\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=880 |
| Status | New |

The variable declared in notify_addr at freebsd-src-2/vnic_dev.c in line 733 is not initialized when it is used by notify at freebsd-src-2/vnic_dev.c in line 703.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vnic_dev.c | freebsd-src-2/vnic_dev.c |
| Line | 735 | 718 |
| Object | notify_addr | notify |

Code Snippet
File Name freebsd-src-2/vnic_dev.c
Method int vnic_dev_notify_set(struct vnic_dev *vdev, u16 intr)

```
....
735.        void *notify_addr = NULL;
```

File Name freebsd-src-2/vnic_dev.c
Method int vnic_dev_notify_setcmd(struct vnic_dev *vdev,

```
....
718.              vdev->notify = notify_addr;
```

**Use of Zero Initialized Pointer\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=881 |
| Status | New |

The variable declared in data at freebsd-src-2/a_object.c in line 239 is not initialized when it is used by data at freebsd-src-2/a_object.c in line 239.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/a_object.c | freebsd-src-2/a_object.c |
| Line | 300 | 299 |
| Object | data | data |

Code Snippet
File Name freebsd-src-2/a_object.c
Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
300.        ret->data = NULL;
....
299.        data = (unsigned char *)ret->data;
```

**Use of Zero Initialized Pointer\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=882 |
| Status | New |

The variable declared in ln at freebsd-src-2/a_object.c in line 239 is not initialized when it is used by ret at freebsd-src-2/a_object.c in line 211.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/a_object.c | freebsd-src-2/a_object.c |
| Line | 323 | 230 |
| Object | ln | ret |

Code Snippet
File Name freebsd-src-2/a_object.c
Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
323.        ret->ln = NULL;
```

File Name freebsd-src-2/a_object.c
Method ASN1_OBJECT *d2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
230.        ret = c2i_ASN1_OBJECT(a, &p, len);
```

**Use of Zero Initialized Pointer\Path 28:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=883 |
| Status | New |

The variable declared in sn at freebsd-src-2/a_object.c in line 239 is not initialized when it is used by ret at freebsd-src-2/a_object.c in line 211.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/a_object.c | freebsd-src-2/a_object.c |
| Line | 322 | 230 |
| Object | sn | ret |

Code Snippet

File Name freebsd-src-2/a_object.c

Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
322.      ret->sn = NULL;
```

File Name freebsd-src-2/a_object.c

Method ASN1_OBJECT *d2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
230.      ret = c2i_ASN1_OBJECT(a, &p, len);
```

**Use of Zero Initialized Pointer\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=884 |
| Status | New |

The variable declared in last at freebsd-src-2/buffer.c in line 795 is not initialized when it is used by first at freebsd-src-2/buffer.c in line 308.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 799 | 315 |
| Object | last | first |

Code Snippet

File Name freebsd-src-2/buffer.c

Method ZERO_CHAIN(struct evbuffer *dst)

```
....
799.        dst->last = NULL;
```

File Name freebsd-src-2/buffer.c

Method evbuffer_chain_insert(struct evbuffer *buf,

```
....
315.            EVUTIL_ASSERT(buf->first == NULL);
```

**Use of Zero Initialized Pointer\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=885 |
| Status | New |

The variable declared in first at freebsd-src-2/buffer.c in line 795 is not initialized when it is used by first at freebsd-src-2/buffer.c in line 308.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 798 | 315 |
| Object | first | first |

Code Snippet

File Name freebsd-src-2/buffer.c

Method ZERO_CHAIN(struct evbuffer *dst)

```
....
798.        dst->first = NULL;
```

File Name freebsd-src-2/buffer.c

Method evbuffer_chain_insert(struct evbuffer *buf,

```
....
315.            EVUTIL_ASSERT(buf->first == NULL);
```

**Use of Zero Initialized Pointer\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=886 |
| Status | New |

The variable declared in Pointer at freebsd-src-2/buffer.c in line 290 is not initialized when it is used by first at freebsd-src-2/buffer.c in line 308.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 299 | 315 |
| Object | Pointer | first |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_free_trailing_empty_chains(struct evbuffer *buf)

```
....
299.              *ch = NULL;
```

File Name freebsd-src-2/buffer.c
Method evbuffer_chain_insert(struct evbuffer *buf,

```
....
315.              EVUTIL_ASSERT(buf->first == NULL);
```

**Use of Zero Initialized Pointer\Path 32:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=887
Status New

The variable declared in Pointer at freebsd-src-2/buffer.c in line 809 is not initialized when it is used by last at freebsd-src-2/buffer.c in line 853.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 817 | 864 |
| Object | Pointer | last |

Code Snippet
File Name freebsd-src-2/buffer.c
Method PRESERVE_PINNED(struct evbuffer *src, struct evbuffer_chain **first,

```
....
817.              *first = *last = NULL;
```

File Name freebsd-src-2/buffer.c

| | |
|---|---|
| Method | RESTORE_PINNED(struct evbuffer *src, struct evbuffer_chain *pinned, |

```
....
864.        src->last = last;
```

**Use of Zero Initialized Pointer\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=888 |
| Status | New |

The variable declared in Pointer at freebsd-src-2/buffer.c in line 809 is not initialized when it is used by first at freebsd-src-2/buffer.c in line 853.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 817 | 863 |
| Object | Pointer | first |

Code Snippet

File Name freebsd-src-2/buffer.c

Method PRESERVE_PINNED(struct evbuffer *src, struct evbuffer_chain **first,

```
....
817.              *first = *last = NULL;
```

File Name freebsd-src-2/buffer.c

Method RESTORE_PINNED(struct evbuffer *src, struct evbuffer_chain *pinned,

```
....
863.        src->first = pinned;
```

**Use of Zero Initialized Pointer\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=889 |
| Status | New |

The variable declared in a at freebsd-src-2/crypto_wolfssl.c in line 1012 is not initialized when it is used by y2 at freebsd-src-2/crypto_wolfssl.c in line 1634.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/crypto_wolfssl.c | freebsd-src-2/crypto_wolfssl.c |

| | | |
|---|---|---|
| Line | 1022 | 1647 |
| Object | a | y2 |

Code Snippet
File Name freebsd-src-2/crypto_wolfssl.c
Method struct crypto_bignum * crypto_bignum_init(void)

```
....
1022.             a = NULL;
```

File Name freebsd-src-2/crypto_wolfssl.c

Method crypto_ec_point_compute_y_sqr(struct crypto_ec *e,

```
....
1647.       y2 = (mp_int *) crypto_bignum_init();
```

**Use of Zero Initialized Pointer\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=890 |
| Status | New |

The variable declared in e at freebsd-src-2/crypto_wolfssl.c in line 1318 is not initialized when it is used by ecdh at freebsd-src-2/crypto_wolfssl.c in line 1699.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/crypto_wolfssl.c | freebsd-src-2/crypto_wolfssl.c |
| Line | 1380 | 1712 |
| Object | e | ecdh |

Code Snippet
File Name freebsd-src-2/crypto_wolfssl.c
Method struct crypto_ec * crypto_ec_init(int group)

```
....
1380.             e = NULL;
```

File Name freebsd-src-2/crypto_wolfssl.c

Method struct crypto_ecdh * crypto_ecdh_init(int group)

```
....
1712.       ecdh->ec = crypto_ec_init(group);
```

**Use of Zero Initialized Pointer\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=891 |
| Status | New |

The variable declared in meth at freebsd-src-2/drbg_lib.c in line 103 is not initialized when it is used by meth at freebsd-src-2/drbg_lib.c in line 470.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/drbg_lib.c | freebsd-src-2/drbg_lib.c |
| Line | 132 | 541 |
| Object | meth | meth |

Code Snippet

File Name freebsd-src-2/drbg_lib.c

Method int RAND_DRBG_set(RAND_DRBG *drbg, int type, unsigned int flags)

```
....
132.          drbg->meth = NULL;
```

File Name freebsd-src-2/drbg_lib.c

Method int rand_drbg_restart(RAND_DRBG *drbg,

```
....
541.              drbg->meth->reseed(drbg, adin, adinlen, NULL, 0);
```

**Use of Zero Initialized Pointer\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=892 |
| Status | New |

The variable declared in meth at freebsd-src-2/drbg_lib.c in line 103 is not initialized when it is used by meth at freebsd-src-2/drbg_lib.c in line 470.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/drbg_lib.c | freebsd-src-2/drbg_lib.c |
| Line | 127 | 541 |
| Object | meth | meth |

Code Snippet

File Name freebsd-src-2/drbg_lib.c

Method int RAND_DRBG_set(RAND_DRBG *drbg, int type, unsigned int flags)

```
....
127.          drbg->meth = NULL;
```

File Name freebsd-src-2/drbg_lib.c

Method int rand_drbg_restart(RAND_DRBG *drbg,

```
....
541.              drbg->meth->reseed(drbg, adin, adinlen, NULL, 0);
```

**Use of Zero Initialized Pointer\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=893 |
| Status | New |

The variable declared in meth at freebsd-src-2/drbg_lib.c in line 103 is not initialized when it is used by meth at freebsd-src-2/drbg_lib.c in line 103.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/drbg_lib.c | freebsd-src-2/drbg_lib.c |
| Line | 132 | 114 |
| Object | meth | meth |

Code Snippet

File Name freebsd-src-2/drbg_lib.c

Method int RAND_DRBG_set(RAND_DRBG *drbg, int type, unsigned int flags)

```
....
132.          drbg->meth = NULL;
....
114.          drbg->meth->uninstantiate(drbg);
```

**Use of Zero Initialized Pointer\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=894 |
| Status | New |

The variable declared in meth at freebsd-src-2/drbg_lib.c in line 103 is not initialized when it is used by meth at freebsd-src-2/drbg_lib.c in line 103.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/drbg_lib.c | freebsd-src-2/drbg_lib.c |

| | | |
|---|---|---|
| Line | 127 | 114 |
| Object | meth | meth |

Code Snippet
File Name freebsd-src-2/drbg_lib.c
Method int RAND_DRBG_set(RAND_DRBG *drbg, int type, unsigned int flags)

```
....
127.          drbg->meth = NULL;
....
114.          drbg->meth->uninstantiate(drbg);
```

**Use of Zero Initialized Pointer\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=895 |
| Status | New |

The variable declared in meth at freebsd-src-2/drbg_lib.c in line 103 is not initialized when it is used by meth at freebsd-src-2/drbg_lib.c in line 377.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/drbg_lib.c | freebsd-src-2/drbg_lib.c |
| Line | 132 | 390 |
| Object | meth | meth |

Code Snippet
File Name freebsd-src-2/drbg_lib.c
Method int RAND_DRBG_set(RAND_DRBG *drbg, int type, unsigned int flags)

```
....
132.          drbg->meth = NULL;
```

File Name freebsd-src-2/drbg_lib.c
Method int RAND_DRBG_uninstantiate(RAND_DRBG *drbg)

```
....
390.      drbg->meth->uninstantiate(drbg);
```

**Use of Zero Initialized Pointer\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=896 |
| Status | New |

The variable declared in meth at freebsd-src-2/drbg_lib.c in line 103 is not initialized when it is used by meth at freebsd-src-2/drbg_lib.c in line 377.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/drbg_lib.c | freebsd-src-2/drbg_lib.c |
| Line | 127 | 390 |
| Object | meth | meth |

Code Snippet
File Name freebsd-src-2/drbg_lib.c
Method int RAND_DRBG_set(RAND_DRBG *drbg, int type, unsigned int flags)

```
....
127.          drbg->meth = NULL;
```

File Name freebsd-src-2/drbg_lib.c
Method int RAND_DRBG_uninstantiate(RAND_DRBG *drbg)

```
....
390.      drbg->meth->uninstantiate(drbg);
```

**Use of Zero Initialized Pointer\Path 42:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=897
Status New

The variable declared in next at freebsd-src-2/dtstream.c in line 230 is not initialized when it is used by last at freebsd-src-2/dtstream.c in line 230.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 257 | 289 |
| Object | next | last |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method dt_msg_queue_submit(struct dt_msg_queue* mq, void* buf, size_t len)

```
....
257.        entry->next = NULL;
....
289.        mq->last = entry;
```

**Use of Zero Initialized Pointer\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=898 |
| Status | New |

The variable declared in next at freebsd-src-2/dtstream.c in line 230 is not initialized when it is used by first at freebsd-src-2/dtstream.c in line 230.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 257 | 287 |
| Object | next | first |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method dt_msg_queue_submit(struct dt_msg_queue* mq, void* buf, size_t len)

```
....
257.        entry->next = NULL;
....
287.              mq->first = entry;
```

**Use of Zero Initialized Pointer\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=899 |
| Status | New |

The variable declared in ep_data at freebsd-src-2/ext2_extents.c in line 1692 is not initialized when it is used by ep_data at freebsd-src-2/ext2_extents.c in line 1692.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1720 | 1728 |
| Object | ep_data | ep_data |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_remove_space(struct inode *ip, off_t length, int flags,

```
....
1720.                   path[i].ep_data = NULL;
....
1728.                       (struct ext4_extent_header
*)path[i].ep_data;
```

**Use of Zero Initialized Pointer\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=900 |
| Status | New |

The variable declared in ep_data at freebsd-src-2/ext2_extents.c in line 575 is not initialized when it is used by ep_data at freebsd-src-2/ext2_extents.c in line 565.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 586 | 568 |
| Object | ep_data | ep_data |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_drop_refs(struct ext4_extent_path *path)

```
....
586.                    path->ep_data = NULL;
```

File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_fill_path_buf(struct ext4_extent_path *path, struct buf *bp)

```
....
568.        KASSERT(path->ep_data != NULL,
```

**Use of Zero Initialized Pointer\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=901 |
| Status | New |

The variable declared in npath at freebsd-src-2/ext2_extents.c in line 1237 is not initialized when it is used by ep_data at freebsd-src-2/ext2_extents.c in line 565.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1247 | 568 |
| Object | npath | ep_data |

Code Snippet
File Name freebsd-src-2/ext2_extents.c

Method ext4_ext_insert_extent(struct inode *ip, struct ext4_extent_path *path,

```
....
1247.        npath = NULL;
```

File Name freebsd-src-2/ext2_extents.c

Method ext4_ext_fill_path_buf(struct ext4_extent_path *path, struct buf *bp)

```
....
568.         KASSERT(path->ep_data != NULL,
```

**Use of Zero Initialized Pointer\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=902 |
| Status | New |

The variable declared in path at freebsd-src-2/ext2_extents.c in line 1396 is not initialized when it is used by ep_data at freebsd-src-2/ext2_extents.c in line 565.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1413 | 568 |
| Object | path | ep_data |

Code Snippet

File Name freebsd-src-2/ext2_extents.c

Method ext4_ext_get_blocks(struct inode *ip, e4fs_daddr_t iblk,

```
....
1413.        path = NULL;
```

File Name freebsd-src-2/ext2_extents.c

Method ext4_ext_fill_path_buf(struct ext4_extent_path *path, struct buf *bp)

```
....
568.         KASSERT(path->ep_data != NULL,
```

**Use of Zero Initialized Pointer\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=903 |
| Status | New |

The variable declared in path at freebsd-src-2/ext2_extents.c in line 1396 is not initialized when it is used by ep_data at freebsd-src-2/ext2_extents.c in line 550.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1413 | 554 |
| Object | path | ep_data |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_get_blocks(struct inode *ip, e4fs_daddr_t iblk,

```
....
1413.        path = NULL;
```

File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_fill_path_bdata(struct ext4_extent_path *path,

```
....
554.        KASSERT(path->ep_data == NULL,
```

**Use of Zero Initialized Pointer\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=904 |
| Status | New |

The variable declared in ep_data at freebsd-src-2/ext2_extents.c in line 575 is not initialized when it is used by ep_data at freebsd-src-2/ext2_extents.c in line 550.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 586 | 554 |
| Object | ep_data | ep_data |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_drop_refs(struct ext4_extent_path *path)

```
....
586.                    path->ep_data = NULL;
```

File Name freebsd-src-2/ext2_extents.c

| | |
|---|---|
| Method | ext4_ext_fill_path_bdata(struct ext4_extent_path *path, |

```
....
554.        KASSERT(path->ep_data == NULL,
```

**Use of Zero Initialized Pointer\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=905 |
| Status | New |

The variable declared in npath at freebsd-src-2/ext2_extents.c in line 1237 is not initialized when it is used by ep_data at freebsd-src-2/ext2_extents.c in line 550.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1247 | 554 |
| Object | npath | ep_data |

Code Snippet

File Name freebsd-src-2/ext2_extents.c

Method ext4_ext_insert_extent(struct inode *ip, struct ext4_extent_path *path,

```
....
1247.       npath = NULL;
```

File Name freebsd-src-2/ext2_extents.c

Method ext4_ext_fill_path_bdata(struct ext4_extent_path *path,

```
....
554.        KASSERT(path->ep_data == NULL,
```

## 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=1060098&projectid=60088&pathid=771 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 451 | 451 |
| Object | item | item |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method int dt_io_thread_register_queue(struct dt_io_thread* dtio,

```
....
451.        struct dt_io_list_item* item = malloc(sizeof(*item));
```

**Memory Leak\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=772
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/val_neg.c | freebsd-src-2/val_neg.c |
| Line | 88 | 88 |
| Object | neg | neg |

Code Snippet
File Name freebsd-src-2/val_neg.c
Method struct val_neg_cache* val_neg_create(struct config_file* cfg, size_t maxiter)

```
....
88.   struct val_neg_cache* neg = (struct val_neg_cache*)calloc(1,
```

**Memory Leak\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=773
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 408 | 408 |
| Object | ad | ad |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
408.        ad = (struct packed_rrset_data*)malloc(s);
```

**Memory Leak\Path 4:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=774
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/diff.c | freebsd-src-2/diff.c |
| Line | 374 | 374 |
| Object | p | p |

Code Snippet
File Name freebsd-src-2/diff.c
Method main(int argc, char **argv)

```
....
374.              if (env != NULL && *env != '\0' && (p = strdup(env)))
{
```

**Memory Leak\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=775
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 361 | 361 |
| Object | socket_path | socket_path |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
361.              dtio->socket_path = strdup(nm);
```

**Memory Leak\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=776 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 374 | 374 |
| Object | ip_str | ip_str |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
374.              dtio->ip_str = strdup(cfg->dnstap_ip);
```

**Memory Leak\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=777 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 386 | 386 |
| Object | tls_server_name | tls_server_name |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
386.                    dtio->tls_server_name = strdup(
```

**Memory Leak\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=778 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 399 | 399 |
| Object | client_key_file | client_key_file |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
399.                    dtio->client_key_file = strdup(
```

**Memory Leak\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=779
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 415 | 415 |
| Object | client_cert_file | client_cert_file |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
415.                    dtio->client_cert_file = strdup(
```

**Memory Leak\Path 10:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=780
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/est.c | freebsd-src-2/est.c |
| Line | 1202 | 1202 |
| Object | fp | fp |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/est.c |
| Method | est_msr_info(device_t dev, uint64_t msr, freq_info **freqs, size_t *freqslen) |

```
....
1202.        fp = malloc(sizeof(freq_info) * 2, M_DEVBUF, M_WAITOK |
M_ZERO);
```

**Memory Leak\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=781 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/if_cpsw.c | freebsd-src-2/if_cpsw.c |
| Line | 869 | 869 |
| Object | nullpad | nullpad |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/if_cpsw.c |
| Method | cpsw_attach(device_t dev) |

```
....
869.        sc->nullpad = malloc(ETHER_MIN_LEN, M_DEVBUF, M_WAITOK |
M_ZERO);
```

**Memory Leak\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=782 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/if_fwe.c | freebsd-src-2/if_fwe.c |
| Line | 309 | 309 |
| Object | bulkxfer | bulkxfer |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/if_fwe.c |
| Method | fwe_init(void *arg) |

```
....
309.              xferq->bulkxfer = (struct fw_bulkxfer *) malloc(
```

**Memory Leak\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=783 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2740 | 2740 |
| Object | ip6po_pktinfo | ip6po_pktinfo |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2740.             dst->ip6po_pktinfo = malloc(sizeof(*dst-
>ip6po_pktinfo),
```

**Memory Leak\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=784 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2747 | 2747 |
| Object | ip6po_nexthop | ip6po_nexthop |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2747.             dst->ip6po_nexthop = malloc(src->ip6po_nexthop-
>sa_len,
```

**Memory Leak\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=785 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2754 | 2754 |
| Object | ip6po_hbh | ip6po_hbh |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2754.        PKTOPT_EXTHDRCPY(ip6po_hbh);
```

**Memory Leak\Path 16:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=786
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2755 | 2755 |
| Object | ip6po_dest1 | ip6po_dest1 |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2755.        PKTOPT_EXTHDRCPY(ip6po_dest1);
```

**Memory Leak\Path 17:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=787
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2756 | 2756 |
| Object | ip6po_dest2 | ip6po_dest2 |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2756.       PKTOPT_EXTHDRCPY(ip6po_dest2);
```

**Memory Leak\Path 18:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=788
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2757 | 2757 |
| Object | ip6po_rthdr | ip6po_rthdr |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2757.       PKTOPT_EXTHDRCPY(ip6po_rthdr); /* not copy the cached route
*/
```

**Memory Leak\Path 19:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=789
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2981 | 2981 |
| Object | ip6po_pktinfo | ip6po_pktinfo |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
2981.                   opt->ip6po_pktinfo = malloc(sizeof(*pktinfo),
```

**Memory Leak\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=790 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3069 | 3069 |
| Object | ip6po_nexthop | ip6po_nexthop |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3069.             opt->ip6po_nexthop = malloc(*buf, M_IP6OPT, M_NOWAIT);
```

**Memory Leak\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=791 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3107 | 3107 |
| Object | ip6po_hbh | ip6po_hbh |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3107.             opt->ip6po_hbh = malloc(hbhlen, M_IP6OPT, M_NOWAIT);
```

**Memory Leak\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=792 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3216 | 3216 |
| Object | ip6po_rthdr | ip6po_rthdr |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3216.             opt->ip6po_rthdr = malloc(rthlen, M_IP6OPT, M_NOWAIT);
```

**Memory Leak\Path 23:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=793
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 1137 | 1137 |
| Object | c | c |

Code Snippet
File Name freebsd-src-2/protocol.c
Method kcm_op_set_default_cache(krb5_context context,

```
....
1137.       c = malloc(sizeof(*c));
```

**Memory Leak\Path 24:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=794
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/protocol.c | freebsd-src-2/protocol.c |
| Line | 1142 | 1142 |
| Object | name | name |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/protocol.c |
| Method | kcm_op_set_default_cache(krb5_context context, |

```
....
1142.        c->name = strdup(name);
```

**Memory Leak\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=795 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 463 | 463 |
| Object | rvp | rvp |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/rt2860.c |
| Method | rt2860_vap_create(struct ieee80211com *ic, const char name[IFNAMSIZ], int unit, |

```
....
463.         rvp = malloc(sizeof(struct rt2860_vap), M_80211_VAP,
M_WAITOK | M_ZERO);
```

**Memory Leak\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=796 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 346 | 346 |
| Object | rai | rai |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/rtsol.c |
| Method | rtsol_input(int sock) |

```
....
346.                ELM_MALLOC(rai, exit(1));
```

**Memory Leak\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=797 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 436 | 436 |
| Object | rao_msg | rao_msg |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
436.                                    rao->rao_msg = strdup(nsbuf);
```

**Memory Leak\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=798 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 495 | 495 |
| Object | rao_msg | rao_msg |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
495.                                    rao->rao_msg = strdup(dname);
```

**Memory Leak\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=799 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 584 | 584 |
| Object | smp3 | smp3 |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method ra_opt_handler(struct ifinfo *ifi)

```
....
584.                            ELM_MALLOC(smp3, goto free2);
```

**Memory Leak\Path 30:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=800
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 621 | 621 |
| Object | smp3 | smp3 |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method ra_opt_handler(struct ifinfo *ifi)

```
....
621.                                ELM_MALLOC(smp3, goto free2);
```

**Memory Leak\Path 31:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=801
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1496 | 1496 |
| Object | dirp | dirp |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/scp.c |
| Method | rsource(char *name, struct stat *statp) |

```
....
1496.       if (!(dirp = opendir(name))) {
```

**Memory Leak\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=802 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/subst.c | freebsd-src-2/subst.c |
| Line | 63 | 63 |
| Object | subst | subst |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/subst.c |
| Method | init_substitution(struct bsdtar *bsdtar) |

```
....
63.   bsdtar->substitution = subst = malloc(sizeof(*subst));
```

**Memory Leak\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=803 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/subst.c | freebsd-src-2/subst.c |
| Line | 83 | 83 |
| Object | rule | rule |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/subst.c |
| Method | add_substitution(struct bsdtar *bsdtar, const char *rule_text) |

```
....
83.   rule = malloc(sizeof(*rule));
```

**Memory Leak\Path 34:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=804 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/subst.c | freebsd-src-2/subst.c |
| Line | 119 | 119 |
| Object | result | result |

Code Snippet
File Name freebsd-src-2/subst.c
Method add_substitution(struct bsdtar *bsdtar, const char *rule_text)

```
....
119.        rule->result = malloc(end_pattern - start_subst + 1);
```

**Memory Leak\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=805 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/subst.c | freebsd-src-2/subst.c |
| Line | 177 | 177 |
| Object | new_str | new_str |

Code Snippet
File Name freebsd-src-2/subst.c
Method realloc_strncat(char **str, const char *append, size_t len)

```
....
177.        new_str = malloc(old_len + len + 1);
```

**Memory Leak\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=806 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_recvmmsg.c | freebsd-src-2/t_recvmmsg.c |

| | | |
|---|---|---|
| Line | 82 | 82 |
| Object | buf | buf |

Code Snippet
File Name freebsd-src-2/t_recvmmsg.c
Method ATF_TC_BODY(recvmmsg_basic, tc)

```
....
82.   buf = malloc(BUFSIZE);
```

**Memory Leak\Path 37:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=807
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_recvmmsg.c | freebsd-src-2/t_recvmmsg.c |
| Line | 86 | 86 |
| Object | mmsghdr | mmsghdr |

Code Snippet
File Name freebsd-src-2/t_recvmmsg.c
Method ATF_TC_BODY(recvmmsg_basic, tc)

```
....
86.   mmsghdr = malloc(sizeof(*mmsghdr) * mmsgcnt);
```

**Memory Leak\Path 38:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=808
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_recvmmsg.c | freebsd-src-2/t_recvmmsg.c |
| Line | 88 | 88 |
| Object | iov | iov |

Code Snippet
File Name freebsd-src-2/t_recvmmsg.c
Method ATF_TC_BODY(recvmmsg_basic, tc)

```
....
88.    iov = malloc(sizeof(*iov) * mmsgcnt);
```

**Memory Leak\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=809 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 537 | 537 |
| Object | argv | argv |

Code Snippet
File Name freebsd-src-2/telnet.c
Method mklist(char *buf, char *name)

```
....
537.        argv = (char **)malloc((n+3)*sizeof(char *));
```

**Memory Leak\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=810 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 4087 | 4087 |
| Object | testprg | testprg |

Code Snippet
File Name freebsd-src-2/test_main.c
Method main(int argc, char **argv)

```
....
4087.            testprg = malloc(testprg_len);
```

**Memory Leak\Path 41:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=811 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 508 | 508 |
| Object | chanlist | chanlist |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_driver_caps(struct wlan_iface *wif)

```
....
508.        wif->chanlist = (struct ieee80211_channel *)malloc(argsize);
```

**Memory Leak\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=812 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 2523 | 2523 |
| Object | data | data |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_mac_acl_macs(struct wlan_iface *wif)

```
....
2523.       if ((data = (uint8_t *)malloc(argsize)) == NULL)
```

**Memory Leak\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=813 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2535 | 2535 |

| | | |
|---|---|---|
| Object | pktopt | pktopt |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_pcbopt(int optname, u_char *buf, int len, struct ip6_pktopts **pktopt,

```
....
2535.             *pktopt = malloc(sizeof(struct ip6_pktopts), M_IP6OPT,
```

**Memory Leak\Path 44:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=814
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3174 | 3174 |
| Object | newdest | newdest |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3174.             *newdest = malloc(destlen, M_IP6OPT, M_NOWAIT);
```

**Memory Leak\Path 45:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=815
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 165 | 165 |
| Object | names | names |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
165.              names[tok-FIRSTTOKEN] = strdup(name);
```

## 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=1060098&projectid=60088&pathid=360 |
| Status | New |

The function s in freebsd-src-2/cachedump.c at line 381 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-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 408 | 408 |
| Object | s | s |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
408.         ad = (struct packed_rrset_data*)malloc(s);
```

**Wrong Size t Allocation\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=361 |
| Status | New |

The function len in freebsd-src-2/cap_sendmsg.c at line 126 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-2/cap_sendmsg.c | freebsd-src-2/cap_sendmsg.c |
| Line | 153 | 153 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/cap_sendmsg.c

| | |
|---|---|
| Method | probe_defrouters(uint32_t ifindex, uint32_t linkid) |

```
....
153.        buf = malloc(len);
```

**Wrong Size t Allocation\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=362 |
| Status | New |

The function sz in freebsd-src-2/krb5_mech.c at line 158 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-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 163 | 163 |
| Object | sz | sz |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/krb5_mech.c |
| Method | get_data(const uint8_t **pp, size_t *lenp, struct krb5_data *dp) |

```
....
163.        dp->kd_data = malloc(sz, M_GSSAPI, M_WAITOK);
```

**Wrong Size t Allocation\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=363 |
| Status | New |

The function mem_sz in freebsd-src-2/tcp_usrreq.c at line 1925 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-2/tcp_usrreq.c | freebsd-src-2/tcp_usrreq.c |
| Line | 1967 | 1967 |
| Object | mem_sz | mem_sz |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/tcp_usrreq.c |
| Method | tcp_set_cc_mod(struct inpcb *inp, struct sockopt *sopt) |

```
....
1967.             ptr = malloc(mem_sz, M_CC_MEM, M_WAITOK);
```

**Wrong Size t Allocation\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=364 |
| Status | New |

The function argsize in freebsd-src-2/wlan_sys.c at line 488 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-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 508 | 508 |
| Object | argsize | argsize |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_driver_caps(struct wlan_iface *wif)

```
....
508.        wif->chanlist = (struct ieee80211_channel *)malloc(argsize);
```

**Wrong Size t Allocation\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=365 |
| Status | New |

The function argsize in freebsd-src-2/wlan_sys.c at line 587 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-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 598 | 598 |
| Object | argsize | argsize |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_channel_list(struct wlan_iface *wif)

```
....
598.        chaninfo = (struct ieee80211req_chaninfo *)malloc(argsize);
```

**Wrong Size t Allocation\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=366 |
| Status | New |

The function argsize in freebsd-src-2/wlan_sys.c at line 2489 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-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 2523 | 2523 |
| Object | argsize | argsize |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_mac_acl_macs(struct wlan_iface *wif)

```
....
2523.       if ((data = (uint8_t *)malloc(argsize)) == NULL)
```

**Wrong Size t Allocation\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=367 |
| Status | New |

The function npos in freebsd-src-2/cut.c at line 225 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-2/cut.c | freebsd-src-2/cut.c |
| Line | 237 | 237 |
| Object | npos | npos |

Code Snippet
File Name freebsd-src-2/cut.c
Method needpos(size_t n)

```
....
237.              if ((positions = realloc(positions, npos)) == NULL)
```

**Wrong Size t Allocation\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=368 |
| Status | New |

The function actual_count in freebsd-src-2/test_main.c at line 1199 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1248 | 1248 |
| Object | actual_count | actual_count |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_contains_lines_any_order(const char *file, int line,

```
....
1248.             actual = calloc(sizeof(char *), actual_count);
```

**Wrong Size t Allocation\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=369 |
| Status | New |

The function buff_size in freebsd-src-2/test_main.c at line 3656 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3666 | 3666 |
| Object | buff_size | buff_size |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3666.       buff = calloc(buff_size, 1);
```

**Wrong Size t Allocation\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=370 |
| Status | New |

The function tried_size in freebsd-src-2/test_main.c at line 3656 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3674 | 3674 |
| Object | tried_size | tried_size |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3674.       tried = calloc(tried_size, 1);
```

**Wrong Size t Allocation\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=371 |
| Status | New |

The function argsize in freebsd-src-2/diff.c at line 469 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-2/diff.c | freebsd-src-2/diff.c |
| Line | 475 | 475 |
| Object | argsize | argsize |

Code Snippet
File Name freebsd-src-2/diff.c
Method set_argstr(char **av, char **ave)

```
....
475.        diffargs = xmalloc(argsize);
```

**Wrong Size t Allocation\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=372 |
| Status | New |

The function need in freebsd-src-2/scp.c at line 1648 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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1816 | 1816 |
| Object | need | need |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1816.                           namebuf = xmalloc(need);
```

**Wrong Size t Allocation\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=373 |
| Status | New |

The function newsize in freebsd-src-2/glob.c at line 675 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-2/glob.c | freebsd-src-2/glob.c |
| Line | 682 | 682 |
| Object | newsize | newsize |

Code Snippet
File Name freebsd-src-2/glob.c
Method globextend(const char *path, glob_t *pglob)

```
....
682.      pathv = xrealloc(pglob->gl_pathv, newsize);
```

**Wrong Size t Allocation\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=374 |
| Status | New |

The function lbuflen in freebsd-src-2/cut.c at line 388 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-2/cut.c | freebsd-src-2/cut.c |
| Line | 403 | 403 |
| Object | lbuflen | lbuflen |

Code Snippet
File Name freebsd-src-2/cut.c
Method f_cut(FILE *fp, const char *fname)

```
....
403.                    mlbuf = malloc(lbuflen + 1);
```

**Wrong Size t Allocation\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=375 |
| Status | New |

The function dirlen in freebsd-src-2/http-server.c at line 159 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-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 235 | 235 |
| Object | dirlen | dirlen |

Code Snippet
File Name freebsd-src-2/http-server.c
Method send_document_cb(struct evhttp_request *req, void *arg)

```
....
235.              pattern = malloc(dirlen+3);
```

**Wrong Size t Allocation\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=376 |
| Status | New |

The function len in freebsd-src-2/t_vnops.c at line 529 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 544 | 544 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method create_nametoolong(const atf_tc_t *tc, const char *mp)

```
....
544.          name = malloc(len+1);
```

**Wrong Size t Allocation\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=377 |
| Status | New |

The function len in freebsd-src-2/t_vnops.c at line 590 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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 608 | 608 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method rename_nametoolong(const atf_tc_t *tc, const char *mp)

```
....
608.        name = malloc(len+1);
```

**Wrong Size t Allocation\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=378 |
| Status | New |

The function len in freebsd-src-2/t_vnops.c at line 642 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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 651 | 651 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method symlink_len(const atf_tc_t *tc, const char *mp, size_t len)

```
....
651.        buf = malloc(len + 1);
```

**Wrong Size t Allocation\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=379 |
| Status | New |

The function expected_count in freebsd-src-2/test_main.c at line 1199 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1225 | 1225 |
| Object | expected_count | expected_count |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_contains_lines_any_order(const char *file, int line,

```
....
1225.             expected = malloc(sizeof(char *) * expected_count);
```

**Wrong Size t Allocation\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=380 |
| Status | New |

The function len in freebsd-src-2/test_main.c at line 1736 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1833 | 1833 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/test_main.c
Method is_symlink(const char *file, int line,

```
....
1833.       linknamew = malloc(len + sizeof(wchar_t));
```

**Wrong Size t Allocation\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=381 |
| Status | New |

The function len in freebsd-src-2/test_main.c at line 1736 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1845 | 1845 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/test_main.c
Method is_symlink(const char *file, int line,

```
....
1845.       contentsw = malloc(len + sizeof(wchar_t));
```

**Wrong Size t Allocation\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=382 |
| Status | New |

The function size in freebsd-src-2/test_main.c at line 2809 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 2841 | 2841 |
| Object | size | size |

Code Snippet
File Name freebsd-src-2/test_main.c
Method sunacl_get(int cmd, int *aclcnt, int fd, const char *path)

```
....
2841.                           aclp = malloc(cnt * size);
```

**Wrong Size t Allocation\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=383 |
| Status | New |

The function size in freebsd-src-2/test_main.c at line 2809 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 2843 | 2843 |
| Object | size | size |

Code Snippet
File Name freebsd-src-2/test_main.c
Method sunacl_get(int cmd, int *aclcnt, int fd, const char *path)

```
....
2843.                          aclp = realloc(NULL, cnt * size);
```

**Wrong Size t Allocation\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=384 |
| Status | New |

The function i in freebsd-src-2/test_main.c at line 1199 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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1234 | 1234 |
| Object | i | i |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_contains_lines_any_order(const char *file, int line,

```
....
1234.                    expected[i] = strdup(lines[i]);
```

**Wrong Size t Allocation\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=385 |
| Status | New |

The function chars in freebsd-src-2/sh.glob.c at line 393 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-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 408 | 408 |
| Object | chars | chars |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method handleone(Char *str, Char **vl, int action)

```
....
408.        str = xmalloc(chars * sizeof(Char));
```

**Wrong Size t Allocation\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=386 |
| Status | New |

The function nslash in freebsd-src-2/scp.c at line 1302 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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1314 | 1314 |
| Object | nslash | nslash |

Code Snippet
File Name freebsd-src-2/scp.c
Method prepare_remote_path(struct sftp_conn *conn, const char *path)

```
....
1314.             return xstrdup(path + 2 + nslash);
```

**Wrong Size t Allocation\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=387 |
| Status | New |

The function i in freebsd-src-2/session.c at line 294 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 303 | 303 |
| Object | i | i |

Code Snippet
File Name freebsd-src-2/session.c
Method set_fwdpermit_from_authopts(struct ssh *ssh, const struct sshauthopt *opts)

```
....
303.                    tmp = cp = xstrdup(auth_opts->permitopen[i]);
```

**Wrong Size t Allocation\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=388 |
| Status | New |

The function i in freebsd-src-2/session.c at line 294 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 318 | 318 |
| Object | i | i |

Code Snippet
File Name freebsd-src-2/session.c
Method set_fwdpermit_from_authopts(struct ssh *ssh, const struct sshauthopt *opts)

```
....
318.                    tmp = cp = xstrdup(auth_opts->permitlisten[i]);
```

**Wrong Size t Allocation\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=389 |
| Status | New |

The function n in freebsd-src-2/session.c at line 982 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-2/session.c | freebsd-src-2/session.c |
| Line | 1121 | 1121 |
| Object | n | n |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
1121.                   ocp = xstrdup(auth_opts->env[n]);
```

**Wrong Size t Allocation\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=390 |
| Status | New |

The function old_len in freebsd-src-2/subst.c at line 167 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-2/subst.c | freebsd-src-2/subst.c |
| Line | 177 | 177 |
| Object | old_len | old_len |

Code Snippet
File Name freebsd-src-2/subst.c
Method realloc_strncat(char **str, const char *append, size_t len)

```
....
177.        new_str = malloc(old_len + len + 1);
```

**Wrong Size t Allocation\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=391 |
| Status | New |

The function len in freebsd-src-2/subst.c at line 167 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-2/subst.c | freebsd-src-2/subst.c |
| Line | 177 | 177 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/subst.c
Method realloc_strncat(char **str, const char *append, size_t len)

```
....
177.        new_str = malloc(old_len + len + 1);
```

**Wrong Size t Allocation\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=392 |
| Status | New |

The function old_len in freebsd-src-2/subst.c at line 189 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-2/subst.c | freebsd-src-2/subst.c |
| Line | 199 | 199 |
| Object | old_len | old_len |

Code Snippet
File Name freebsd-src-2/subst.c
Method realloc_strcat(char **str, const char *append)

```
....
199.        new_str = malloc(old_len + strlen(append) + 1);
```

## 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=1060098&projectid=60088&pathid=398 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 239 of freebsd-src-2/a_object.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-2/a_object.c | freebsd-src-2/a_object.c |
| Line | 258 | 258 |

| | | |
|---|---|---|
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/a_object.c
Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
258.      length = (int)len;
```

**Integer Overflow\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=399 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1255 of freebsd-src-2/buffer.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-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1283 | 1283 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_remove_buffer(struct evbuffer *src, struct evbuffer *dst,

```
....
1283.             result = (int)datlen; /*XXXX should return
ev_ssize_t*/
```

**Integer Overflow\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=400 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1255 of freebsd-src-2/buffer.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-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1337 | 1337 |
| Object | AssignExpr | AssignExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_remove_buffer(struct evbuffer *src, struct evbuffer *dst, |

```
....
1337.       result = (int)nread;/*XXXX should change return type */
```

**Integer Overflow\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=401 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2271 of freebsd-src-2/buffer.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-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 2331 | 2331 |
| Object | AssignExpr | AssignExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_read(struct evbuffer *buf, evutil_socket_t fd, int howmuch) |

```
....
2331.                           n = bytesRead;
```

**Integer Overflow\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=402 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2403 of freebsd-src-2/buffer.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-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 2444 | 2444 |
| Object | AssignExpr | AssignExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_write_iovec(struct evbuffer *buffer, evutil_socket_t fd, |

```
....
2444.                   n = bytesSent;
```

**Integer Overflow\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=403 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1081 of freebsd-src-2/crypto_wolfssl.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-2/crypto_wolfssl.c | freebsd-src-2/crypto_wolfssl.c |
| Line | 1096 | 1096 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/crypto_wolfssl.c
Method int crypto_bignum_to_bin(const struct crypto_bignum *a,

```
....
1096.             offset = padlen - num_bytes;
```

**Integer Overflow\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=404 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 340 of freebsd-src-2/cut.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-2/cut.c | freebsd-src-2/cut.c |
| Line | 349 | 349 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/cut.c
Method c_cut(FILE *fp, const char *fname)

```
....
349.             for (col = maxval; col; --col) {
```

**Integer Overflow\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=405 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 388 of freebsd-src-2/cut.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-2/cut.c | freebsd-src-2/cut.c |
| Line | 434 | 434 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/cut.c
Method f_cut(FILE *fp, const char *fname)

```
....
434.                for (field = maxval, p = lbuf; field; --field, ++pos)
{
```

**Integer Overflow\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=406 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 129 of freebsd-src-2/diff.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-2/diff.c | freebsd-src-2/diff.c |
| Line | 174 | 174 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/diff.c
Method main(int argc, char **argv)

```
....
174.                            diff_context = (int)l;
```

**Integer Overflow\Path 10:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=407 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 129 of freebsd-src-2/diff.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-2/diff.c | freebsd-src-2/diff.c |
| Line | 273 | 273 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/diff.c
Method main(int argc, char **argv)

```
....
273.                            diff_context = (int)l;
```

**Integer Overflow\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=408 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 678 of freebsd-src-2/e_aria.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-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 739 | 739 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_ccm_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
739.                        rv = len;
```

**Integer Overflow\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=409 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 393 of freebsd-src-2/e_aria.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-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 426 | 426 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
426.           rv = len + EVP_GCM_TLS_EXPLICIT_IV_LEN +
EVP_GCM_TLS_TAG_LEN;
```

**Integer Overflow\Path 13:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=410
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 393 of freebsd-src-2/e_aria.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-2/e_aria.c | freebsd-src-2/e_aria.c |
| Line | 440 | 440 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/e_aria.c
Method static int aria_gcm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
440.           rv = len;
```

**Integer Overflow\Path 14:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=411
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 65 of freebsd-src-2/e_rc4_hmac_md5.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-2/e_rc4_hmac_md5.c | freebsd-src-2/e_rc4_hmac_md5.c |
| Line | 143 | 143 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/e_rc4_hmac_md5.c
Method static int rc4_hmac_md5_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
143.                l = (key->md.Nl + (blocks << 3)) & 0xffffffffU;
```

**Integer Overflow\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=412 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1550 of freebsd-src-2/ext2_extents.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-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1584 | 1584 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_rm_leaf(struct inode *ip, struct ext4_extent_path *path,

```
....
1584.                a = ex_blk > start ? ex_blk : start;
```

**Integer Overflow\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=413 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1550 of freebsd-src-2/ext2_extents.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-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1585 | 1585 |

| | | |
|---|---|---|
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_rm_leaf(struct inode *ip, struct ext4_extent_path *path,

```
....
1585.             b = (uint64_t)ex_blk + ex_len - 1 <
```

**Integer Overflow\Path 17:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=414
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1550 of freebsd-src-2/ext2_extents.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-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1592 | 1592 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_rm_leaf(struct inode *ip, struct ext4_extent_path *path,

```
....
1592.                     block = ex_blk;
```

**Integer Overflow\Path 18:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=415
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1550 of freebsd-src-2/ext2_extents.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-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1599 | 1599 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/ext2_extents.c

| | |
|---|---|
| Method | ext4_ext_rm_leaf(struct inode *ip, struct ext4_extent_path *path, |

```
....
1599.                   block = ex_blk;
```

**Integer Overflow\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=416 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1399 of freebsd-src-2/krb5_mech.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-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1431 | 1431 |
| Object | AssignExpr | AssignExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/krb5_mech.c |
| Method | krb5_wrap_new(struct krb5_context *kc, int conf_req_flag, |

```
....
1431.                   EC = mlen % mblen;
```

**Integer Overflow\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=417 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1399 of freebsd-src-2/krb5_mech.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-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1468 | 1468 |
| Object | AssignExpr | AssignExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/krb5_mech.c |
| Method | krb5_wrap_new(struct krb5_context *kc, int conf_req_flag, |

```
....
1468.               EC = cklen;
```

**Integer Overflow\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=418 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 455 of freebsd-src-2/mem_dbg.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-2/mem_dbg.c | freebsd-src-2/mem_dbg.c |
| Line | 532 | 532 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/mem_dbg.c
Method static void print_leak(const MEM *m, MEM_LEAK *l)

```
....
532.              buf_len = ami_cnt + n;
```

**Integer Overflow\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=419 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1648 of freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1891 | 1891 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1891.                          amt -= j;
```

**Integer Overflow\Path 23:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=420 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 227 of freebsd-src-2/sh.glob.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-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 258 | 258 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method expbrace(Char ***nvp, Char ***elp, int size)

```
....
258.              size += GLOBSPACE > l ? GLOBSPACE : l;
```

**Integer Overflow\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=421 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2489 of freebsd-src-2/wlan_sys.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-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 2530 | 2530 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_get_mac_acl_macs(struct wlan_iface *wif)

```
....
2530.       nacls = argsize / sizeof(*acllist);
```

**Integer Overflow\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=422 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3036 of freebsd-src-2/wlan_sys.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-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 3049 | 3049 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_mesh_get_routelist(struct wlan_iface *wif)

```
....
3049.       nroutes = argsize / sizeof(*rt);
```

## 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=1060098&projectid=60088&pathid=740
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/acpi_thermal.c | freebsd-src-2/acpi_thermal.c |
| Line | 985 | 985 |
| Object | sc | sc |

Code Snippet
File Name freebsd-src-2/acpi_thermal.c
Method acpi_tz_thread(void *arg)

```
....
985.                free(sc, M_TEMP);
```

**Double Free\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=741
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1761 | 1777 |
| Object | M_EXT2EXTENTS | M_EXT2EXTENTS |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_remove_space(struct inode *ip, off_t length, int flags,

```
....
1761.                   free(path[i].ep_data, M_EXT2EXTENTS);
....
1777.       free(path, M_EXT2EXTENTS);
```

**Double Free\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=742
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1719 | 1777 |
| Object | M_EXT2EXTENTS | M_EXT2EXTENTS |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_remove_space(struct inode *ip, off_t length, int flags,

```
....
1719.                   free(path[i].ep_data, M_EXT2EXTENTS);
....
1777.       free(path, M_EXT2EXTENTS);
```

**Double Free\Path 4:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=743
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 967 | 977 |

| | | |
|---|---|---|
| Object | cp | cp |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
967.                    free(cp);
....
977.                    free(cp);
```

**Double Free\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=744
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 967 | 989 |
| Object | cp | cp |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
967.                    free(cp);
....
989.                    free(cp);
```

**Double Free\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=745
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 977 | 989 |
| Object | cp | cp |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
977.                    free(cp);
....
989.                    free(cp);
```

**Double Free\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=746 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 989 | 992 |
| Object | cp | cp |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
989.                    free(cp);
....
992.                free(cp);
```

**Double Free\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=747 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 967 | 992 |
| Object | cp | cp |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
967.                    free(cp);
....
992.                free(cp);
```

**Double Free\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=748 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 977 | 992 |
| Object | cp | cp |

Code Snippet
File Name freebsd-src-2/scp.c
Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
977.                    free(cp);
....
992.                free(cp);
```

**Double Free\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=749 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1125 | 1131 |
| Object | bp | bp |

Code Snippet
File Name freebsd-src-2/scp.c
Method toremote(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1125.                           free(bp);
....
1131.                           free(bp);
```

**Double Free\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=750 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1205 | 1205 |
| Object | bp | bp |

Code Snippet
File Name freebsd-src-2/scp.c
Method toremote(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1205.                           free(bp);
```

**Double Free\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=751 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1063 | 1217 |
| Object | host | host |

Code Snippet
File Name freebsd-src-2/scp.c
Method toremote(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1063.                free(host);
....
1217.        free(host);
```

**Double Free\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=752 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |

| | | |
|---|---|---|
| Line | 1064 | 1218 |
| Object | src | src |

Code Snippet
File Name freebsd-src-2/scp.c
Method toremote(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1064.              free(src);
....
1218.        free(src);
```

**Double Free\Path 14:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=753
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1290 | 1290 |
| Object | bp | bp |

Code Snippet
File Name freebsd-src-2/scp.c
Method tolocal(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1290.              free(bp);
```

**Double Free\Path 15:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=754
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1233 | 1295 |
| Object | suser | suser |

Code Snippet
File Name freebsd-src-2/scp.c
Method tolocal(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1233.              free(suser);
....
1295.        free(suser);
```

**Double Free\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=755 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1234 | 1296 |
| Object | host | host |

Code Snippet
File Name freebsd-src-2/scp.c
Method tolocal(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1234.              free(host);
....
1296.        free(host);
```

**Double Free\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=756 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1235 | 1297 |
| Object | src | src |

Code Snippet
File Name freebsd-src-2/scp.c
Method tolocal(int argc, char **argv, enum scp_mode_e mode, char *sftp_direct)

```
....
1235.              free(src);
....
1297.        free(src);
```

**Double Free\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=757 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 967 | 1958 |
| Object | cp | patterns |

Code Snippet

File Name freebsd-src-2/scp.c

Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
967.                    free(cp);
```

File Name freebsd-src-2/scp.c

Method sink(int argc, char **argv, const char *src)

```
....
1958.       free(patterns);
```

**Double Free\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=758 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 977 | 1958 |
| Object | cp | patterns |

Code Snippet

File Name freebsd-src-2/scp.c

Method brace_expand(const char *pattern, char ***patternsp, size_t *npatternsp)

```
....
977.                    free(cp);
```

| | |
|---|---|
| File Name | freebsd-src-2/scp.c |
| Method | sink(int argc, char **argv, const char *src) |

```
....
1958.        free(patterns);
```

**Double Free\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=759 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 957 | 968 |
| Object | var_name | var_name |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/session.c |
| Method | copy_environment_denylist(char **source, char ***env, u_int *envsize, |

```
....
957.                    free(var_name);
....
968.                free(var_name);
```

**Double Free\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=760 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/subst.c | freebsd-src-2/subst.c |
| Line | 279 | 279 |
| Object | Pointer | Pointer |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/subst.c |
| Method | apply_substitution(struct bsdtar *bsdtar, const char *name, char **result, |

```
....
279.                                        free(*result);
```

## Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

### Categories

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

*Description*

**Use of Uninitialized Variable\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=835 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/openpic.c | freebsd-src-2/openpic.c |
| Line | 249 | 253 |
| Object | cpu | cpu |

Code Snippet
File Name freebsd-src-2/openpic.c
Method int cpu, ncpu;

```
....
249.              int cpu, ncpu;
```

File Name freebsd-src-2/openpic.c
Method CPU_FOREACH(cpu) {

```
....
253.                    if (!(mask & (1 << cpu)))
```

**Use of Uninitialized Variable\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=836 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |

| | | |
|---|---|---|
| Line | 66 | 1663 |
| Object | crmod | crmod |

Code Snippet
File Name freebsd-src-2/telnet.c
Method crmod,

```
....
66.    crmod,
```

File Name freebsd-src-2/telnet.c

Method telrcv(void)

```
....
1663.                    if (crmod) {
```

**Use of Uninitialized Variable\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=837
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 66 | 1623 |
| Object | crmod | crmod |

Code Snippet
File Name freebsd-src-2/telnet.c
Method crmod,

```
....
66.    crmod,
```

File Name freebsd-src-2/telnet.c

Method telrcv(void)

```
....
1623.            else if ((c == '\n') &&
my_want_state_is_dont(TELOPT_ECHO) && !crmod) {
```

**Use of Uninitialized Variable\Path 4:**

Severity Medium

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=838 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 66 | 1670 |
| Object | crmod | crmod |

Code Snippet

File Name freebsd-src-2/telnet.c

Method crmod,

```
....
66.    crmod,
```

File Name freebsd-src-2/telnet.c

Method telrcv(void)

```
....
1670.                   if (crmod) {
```

**Use of Uninitialized Variable\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=839 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 68 | 1944 |
| Object | crlf | crlf |

Code Snippet

File Name freebsd-src-2/telnet.c

Method crlf, /* Should '\r' be mapped to <CR><LF> (or <CR><NUL>)? */

```
....
68.    crlf,        /* Should '\r' be mapped to <CR><LF> (or <CR><NUL>)?
*/
```

File Name freebsd-src-2/telnet.c

| | |
|---|---|
| Method | telsnd() |

```
....
1944.              if (!crlf) {
```

**Use of Uninitialized Variable\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=840 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 69 | 2084 |
| Object | telnetport | telnetport |

Code Snippet

File Name freebsd-src-2/telnet.c

Method telnetport,

```
....
69.   telnetport,
```

File Name freebsd-src-2/telnet.c

Method my_telnet(char *user)

```
....
2084.      if (telnetport && wantencryption) {
```

**Use of Uninitialized Variable\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=841 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 69 | 2055 |
| Object | telnetport | telnetport |

Code Snippet

File Name freebsd-src-2/telnet.c

Method telnetport,

```
....
69.   telnetport,
```

File Name freebsd-src-2/telnet.c

Method my_telnet(char *user)

```
....
2055.      if (telnetport) {
```

**Use of Uninitialized Variable\Path 8:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=842
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 74 | 2320 |
| Object | autosynch | autosynch |

Code Snippet
File Name freebsd-src-2/telnet.c
Method autosynch,  /* send interrupt characters with SYNCH? */

```
....
74.   autosynch,  /* send interrupt characters with SYNCH? */
```

File Name freebsd-src-2/telnet.c

Method sendbrk(void)

```
....
2320.      if (autosynch) {
```

**Use of Uninitialized Variable\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=843
Status New

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 74 | 2306 |
| Object | autosynch | autosynch |

Code Snippet
File Name freebsd-src-2/telnet.c
Method autosynch, /* send interrupt characters with SYNCH? */

```
....
74.   autosynch,  /* send interrupt characters with SYNCH? */
```

File Name freebsd-src-2/telnet.c
Method intp(void)

```
....
2306.       if (autosynch) {
```

**Use of Uninitialized Variable\Path 10:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=844
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 74 | 2334 |
| Object | autosynch | autosynch |

Code Snippet
File Name freebsd-src-2/telnet.c
Method autosynch, /* send interrupt characters with SYNCH? */

```
....
74.   autosynch,  /* send interrupt characters with SYNCH? */
```

File Name freebsd-src-2/telnet.c
Method sendabort(void)

```
....
2334.       if (autosynch) {
```

**Use of Uninitialized Variable\Path 11:**

Severity Medium

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=845 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 74 | 2348 |
| Object | autosynch | autosynch |

Code Snippet
File Name freebsd-src-2/telnet.c
Method autosynch, /* send interrupt characters with SYNCH? */

```
....
74.   autosynch,  /* send interrupt characters with SYNCH? */
```

File Name freebsd-src-2/telnet.c
Method sendsusp(void)

```
....
2348.       if (autosynch) {
```

**Use of Uninitialized Variable\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=846 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 44 | 309 |
| Object | verbose | verbose |

Code Snippet
File Name freebsd-src-2/valectl.c
Method int verbose;

```
....
44.  int verbose;
```

File Name freebsd-src-2/valectl.c

Method bdg_ctl(struct args *a)

```
....
309.              if (verbose) {
```

**Use of Uninitialized Variable\Path 13:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=847
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 44 | 430 |
| Object | verbose | verbose |

Code Snippet
File Name freebsd-src-2/valectl.c
Method int verbose;

```
....
44.  int verbose;
```

File Name freebsd-src-2/valectl.c
Method main(int argc, char *argv[])

```
....
430.                    verbose++;
```

**Use of Uninitialized Variable\Path 14:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=848
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 44 | 315 |
| Object | verbose | verbose |

Code Snippet
File Name freebsd-src-2/valectl.c

| | |
|---|---|
| Method | int verbose; |

```
....
44.  int verbose;
```

| | |
|---|---|
| File Name | freebsd-src-2/valectl.c |
| Method | bdg_ctl(struct args *a) |

```
....
315.              if (verbose) {
```

**Use of Uninitialized Variable\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=849 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 44 | 321 |
| Object | verbose | verbose |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/valectl.c |
| Method | int verbose; |

```
....
44.  int verbose;
```

| | |
|---|---|
| File Name | freebsd-src-2/valectl.c |
| Method | bdg_ctl(struct args *a) |

```
....
321.              if (verbose) {
```

**Use of Uninitialized Variable\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=850 |
| Status | New |

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 197 | 1396 |
| Object | vga_sub_configure | vga_sub_configure |

Code Snippet
File Name freebsd-src-2/vga.c
Method int (*vga_sub_configure)(int flags);

```
....
197.        int             (*vga_sub_configure)(int flags);
```

File Name freebsd-src-2/vga.c

Method vga_init(int unit, video_adapter_t *adp, int flags)

```
....
1396.      if (vga_sub_configure != NULL)
```

**Use of Uninitialized Variable\Path 17:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=851
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 197 | 485 |
| Object | vga_sub_configure | vga_sub_configure |

Code Snippet
File Name freebsd-src-2/vga.c
Method int (*vga_sub_configure)(int flags);

```
....
197.        int             (*vga_sub_configure)(int flags);
```

File Name freebsd-src-2/vga.c

Method vga_configure(int flags)

```
....
485.      if (vga_sub_configure != NULL)
```

**Use of Uninitialized Variable\Path 18:**

Severity Medium

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=852 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 765 | 960 |
| Object | rfr_78 | rfr_78 |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_init_bcm2050(struct bwi_mac *mac)

```
....
765.         uint16_t phyr_35, phyr_30 = 0, rfr_78, phyr_80f = 0,
phyr_810 = 0;
....
960.                 rf->rf_calib = rfr_78;
```

**Use of Uninitialized Variable\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=853 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 2771 | 2829 |
| Object | sigbytes2 | sigbytes2 |

Code Snippet
File Name freebsd-src-2/statem_srvr.c
Method int tls_construct_server_key_exchange(SSL *s, WPACKET *pkt)

```
....
2771.           unsigned char *sigbytes1, *sigbytes2, *tbs;
....
2829.                || sigbytes1 != sigbytes2) {
```

**Use of Uninitialized Variable\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=854 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 1298 | 1302 |
| Object | cookie_leni | cookie_leni |

Code Snippet
File Name freebsd-src-2/statem_srvr.c
Method int dtls_construct_hello_verify_request(SSL *s, WPACKET *pkt)

```
....
1298.       unsigned int cookie_leni;
....
1302.           cookie_leni > 255) {
```

**Use of Uninitialized Variable\Path 21:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=855
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 1259 | 1263 |
| Object | msglen | msglen |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method int dtls1_close_construct_packet(SSL *s, WPACKET *pkt, int htype)

```
....
1259.       size_t msglen;
....
1263.               || msglen > INT_MAX)
```

## 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=1060098&projectid=60088&pathid=816 |
| Status | New |

The variable declared in hbh at freebsd-src-2/ip6_output.c in line 1322 is not initialized when it is used by ip6h_len at freebsd-src-2/ip6_output.c in line 1322.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 1345 | 1390 |
| Object | hbh | ip6h_len |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_insert_jumboopt(struct ip6_exthdrs *exthdrs, u_int32_t plen)

```
....
1345.             struct ip6_hbh *hbh;
....
1390.             hbh->ip6h_len += (JUMBOOPTLEN >> 3);
```

**Use of Uninitialized Pointer\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=817 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by flags at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 608 |
| Object | strtmp | flags |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
608.              && (strtmp->flags & ASN1_STRING_FLAG_NDEF)) {
```

**Use of Uninitialized Pointer\Path 3:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=818 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by type at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 532 |
| Object | strtmp | type |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
532.          utype = strtmp->type;
```

**Use of Uninitialized Pointer\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=819 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by data at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 610 |
| Object | strtmp | data |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
610.                  strtmp->data = cout;
```

**Use of Uninitialized Pointer\Path 5:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=820 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by length at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 611 |
| Object | strtmp | length |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
611.                  strtmp->length = 0;
```

**Use of Uninitialized Pointer\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=821 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by data at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 616 |
| Object | strtmp | data |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
616.          cont = strtmp->data;
```

**Use of Uninitialized Pointer\Path 7:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=822 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by length at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 617 |
| Object | strtmp | length |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
617.          len = strtmp->length;
```

**Use of Uninitialized Pointer\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=823 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by flags at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 608 |
| Object | strtmp | flags |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
608.              && (strtmp->flags & ASN1_STRING_FLAG_NDEF)) {
```

**Use of Uninitialized Pointer\Path 9:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=824 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by data at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 610 |
| Object | strtmp | data |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
610.                  strtmp->data = cout;
```

**Use of Uninitialized Pointer\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=825 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by length at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 611 |
| Object | strtmp | length |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
611.                  strtmp->length = 0;
```

**Use of Uninitialized Pointer\Path 11:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=826 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by data at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 616 |
| Object | strtmp | data |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
616.          cont = strtmp->data;
```

**Use of Uninitialized Pointer\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=827 |
| Status | New |

The variable declared in strtmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by length at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 511 | 617 |
| Object | strtmp | length |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
511.      ASN1_STRING *strtmp;
....
617.          len = strtmp->length;
```

**Use of Uninitialized Pointer\Path 13:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=828 |
| Status | New |

The variable declared in otmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by length at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 512 | 548 |
| Object | otmp | length |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
512.      ASN1_OBJECT *otmp;
....
548.          len = otmp->length;
```

**Use of Uninitialized Pointer\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=829 |
| Status | New |

The variable declared in otmp at freebsd-src-2/tasn_enc.c in line 507 is not initialized when it is used by data at freebsd-src-2/tasn_enc.c in line 507.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 512 | 547 |
| Object | otmp | data |

Code Snippet
File Name freebsd-src-2/tasn_enc.c
Method static int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
512.      ASN1_OBJECT *otmp;
....
547.          cont = otmp->data;
```

**Use of Uninitialized Pointer\Path 15:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=830 |
| Status | New |

The variable declared in sw at freebsd-src-2/vga.c in line 76 is not initialized when it is used by sw at freebsd-src-2/vga.c in line 76.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 79 | 85 |
| Object | sw | sw |

Code Snippet
File Name freebsd-src-2/vga.c
Method vga_probe_unit(int unit, video_adapter_t *buf, int flags)

```
....
79.   video_switch_t *sw;
....
85.   error = (*sw->probe)(unit, &adp, NULL, flags);
```

**Use of Uninitialized Pointer\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=831 |
| Status | New |

The variable declared in sw at freebsd-src-2/vga.c in line 76 is not initialized when it is used by sw at freebsd-src-2/vga.c in line 76.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 79 | 83 |
| Object | sw | sw |

Code Snippet
File Name freebsd-src-2/vga.c
Method vga_probe_unit(int unit, video_adapter_t *buf, int flags)

```
....
79.   video_switch_t *sw;
....
83.   if (sw == NULL)
```

**Use of Uninitialized Pointer\Path 17:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=832 |
| Status | New |

The variable declared in sw at freebsd-src-2/vga.c in line 93 is not initialized when it is used by sw at freebsd-src-2/vga.c in line 93.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 95 | 102 |
| Object | sw | sw |

Code Snippet
File Name freebsd-src-2/vga.c
Method vga_attach_unit(int unit, vga_softc_t *sc, int flags)

```
....
95.    video_switch_t *sw;
....
102.         error = (*sw->probe)(unit, &sc->adp, NULL, flags);
```

**Use of Uninitialized Pointer\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=833 |
| Status | New |

The variable declared in sw at freebsd-src-2/vga.c in line 93 is not initialized when it is used by sw at freebsd-src-2/vga.c in line 93.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 95 | 99 |
| Object | sw | sw |

Code Snippet
File Name freebsd-src-2/vga.c
Method vga_attach_unit(int unit, vga_softc_t *sc, int flags)

```
....
95.    video_switch_t *sw;
....
99.    if (sw == NULL)
```

**Use of Uninitialized Pointer\Path 19:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=834 |
| Status | New |

The variable declared in sw at freebsd-src-2/vga.c in line 93 is not initialized when it is used by sw at freebsd-src-2/vga.c in line 93.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 95 | 105 |
| Object | sw | sw |

Code Snippet
File Name freebsd-src-2/vga.c
Method vga_attach_unit(int unit, vga_softc_t *sc, int flags)

```
....
95.   video_switch_t *sw;
....
105.        return (*sw->init)(unit, sc->adp, flags);
```

## 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=1060098&projectid=60088&pathid=764 |
| Status | New |

Method *pwd; at line 443 of freebsd-src-2/scp.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 443 | 443 |
| Object | pwd | pwd |

Code Snippet
File Name freebsd-src-2/scp.c
Method struct passwd *pwd;

```
....
443.  struct passwd *pwd;
```

**Heap Inspection\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=765 |
| Status | New |

Method main at line 3860 of freebsd-src-2/test_main.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3887 | 3887 |
| Object | pwd | pwd |

Code Snippet
File Name freebsd-src-2/test_main.c
Method main(int argc, char **argv)

```
....
3887.       char *pwd, *testprogdir, *tmp2 = NULL, *vlevel = NULL;
```

**Heap Inspection\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=766 |
| Status | New |

Method get_refdir at line 3656 of freebsd-src-2/test_main.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3659 | 3659 |
| Object | pwd | pwd |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3659.       char *buff, *tried, *pwd = NULL, *p = NULL;
```

**Heap Inspection\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=767 |
| Status | New |

Method main at line 3860 of freebsd-src-2/test_main.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3943 | 3942 |
| Object | pwd | realloc |

Code Snippet
File Name freebsd-src-2/test_main.c
Method main(int argc, char **argv)

```
....
3943.                   strlen(pwd) + 1 + strlen(testprogdir) + 1)) ==
NULL)
....
3942.             if ((testprogdir = (char *)realloc(testprogdir,
```

**Heap Inspection\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=768 |
| Status | New |

Method main at line 3860 of freebsd-src-2/test_main.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3898 | 3942 |
| Object | pwd | realloc |

Code Snippet
File Name freebsd-src-2/test_main.c
Method main(int argc, char **argv)

```
....
3898.       while (pwd[strlen(pwd) - 1] == '\n')
....
3942.             if ((testprogdir = (char *)realloc(testprogdir,
```

**Heap Inspection\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=769 |
| Status | New |

Method main at line 3860 of freebsd-src-2/test_main.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3894 | 3942 |
| Object | pwd | realloc |

Code Snippet
File Name freebsd-src-2/test_main.c
Method main(int argc, char **argv)

```
....
3894.       pwd = getcwd(NULL, PATH_MAX);/* Solaris getcwd needs the
size. */
....
3942.             if ((testprogdir = (char *)realloc(testprogdir,
```

**Heap Inspection\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=770 |
| Status | New |

Method main at line 3860 of freebsd-src-2/test_main.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3899 | 3942 |
| Object | pwd | realloc |

Code Snippet
File Name freebsd-src-2/test_main.c

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

```
....
3899.             pwd[strlen(pwd) - 1] = '\0';
....
3942.             if ((testprogdir = (char *)realloc(testprogdir,
```

## 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=1060098&projectid=60088&pathid=206 |
| Status | New |

The application performs an illegal operation in ar9300_aic_cal_post_process, in freebsd-src-2/ar9300_aic.c. In line 282, 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 ar9300_aic_cal_post_process of freebsd-src-2/ar9300_aic.c, at line 282.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ar9300_aic.c | freebsd-src-2/ar9300_aic.c |
| Line | 363 | 363 |
| Object | BinaryExpr | BinaryExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/ar9300_aic.c |
| Method | ar9300_aic_cal_post_process (struct ath_hal *ah) |

```
....
363.                         (end_idx - i) +
```

**Divide By Zero\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=207 |
| Status | New |

The application performs an illegal operation in ar9300_aic_cal_post_process, in freebsd-src-2/ar9300_aic.c. In line 282, 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 ar9300_aic_cal_post_process of freebsd-src-2/ar9300_aic.c, at line 282.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/ar9300_aic.c | freebsd-src-2/ar9300_aic.c |
| Line | 369 | 369 |
| Object | BinaryExpr | BinaryExpr |

Code Snippet
File Name freebsd-src-2/ar9300_aic.c
Method ar9300_aic_cal_post_process (struct ath_hal *ah)

```
....
369.                        (end_idx - i) +
```

**Divide By Zero\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=208 |
| Status | New |

The application performs an illegal operation in bwi_rf_calc_nrssi_slope_11g, in freebsd-src-2/bwirf.c. In line 1905, 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 bwi_rf_calc_nrssi_slope_11g of freebsd-src-2/bwirf.c, at line 1905.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 2033 | 2033 |
| Object | BinaryExpr | BinaryExpr |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_calc_nrssi_slope_11g(struct bwi_mac *mac)

```
....
2033.            rf->rf_nrssi_slope = 0x400000 / (nrssi[0] - nrssi[1]);
```

**Divide By Zero\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=209 |
| Status | New |

The application performs an illegal operation in server_update, in freebsd-src-2/server.c. In line 72, the program attempts to divide by server_limit, 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 server_limit in server_update of freebsd-src-2/server.c, at line 72.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/server.c | freebsd-src-2/server.c |
| Line | 80 | 80 |
| Object | server_limit | server_limit |

Code Snippet
File Name freebsd-src-2/server.c
Method server_update(int count)

```
....
80.   server_avail = UINT8_MAX - (count - 1) * UINT8_MAX / server_limit;
```

## 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=1060098&projectid=60088&pathid=197
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2729 of freebsd-src-2/if_cpsw.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-2/if_cpsw.c | freebsd-src-2/if_cpsw.c |
| Line | 2760 | 2760 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/if_cpsw.c
Method cpsw_add_sysctls(struct cpsw_softc *sc)

```
....
2760.             port[0] = '0' + i;
```

**Char Overflow\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=198

| Status | New |
|---|---|

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 351 of freebsd-src-2/telnet.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-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 397 | 397 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/telnet.c
Method dooption(int option)

```
....
397.              telopt_environ = option;
```

**Char Overflow\Path 3:**

| Severity | Medium |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=199 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1043 of freebsd-src-2/telnet.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-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1052 | 1052 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_mode(unsigned char *cmd, int len, int init)

```
....
1052.       str_lm_mode[4] = linemode;
```

## Path Traversal

Query Path:
CPP\Cx\CPP Medium Threat\Path Traversal Version:0

### Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

*Description*

**Path Traversal\Path 1:**

| Severity | Medium |
|---|---|

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=761 |
| Status | New |

Method main at line 78 of freebsd-src-2/cut.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 78 of freebsd-src-2/cut.c. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cut.c | freebsd-src-2/cut.c |
| Line | 78 | 149 |
| Object | argv | Pointer |

Code Snippet
File Name freebsd-src-2/cut.c
Method main(int argc, char *argv[])

```
....
78.  main(int argc, char *argv[])
....
149.                            if (!(fp = fopen(*argv, "r"))) {
```

**Path Traversal\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=762 |
| Status | New |

Method main at line 78 of freebsd-src-2/cut.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 78 of freebsd-src-2/cut.c. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cut.c | freebsd-src-2/cut.c |
| Line | 78 | 149 |
| Object | argv | argv |

Code Snippet
File Name freebsd-src-2/cut.c
Method main(int argc, char *argv[])

```
....
78.  main(int argc, char *argv[])
....
149.                            if (!(fp = fopen(*argv, "r"))) {
```

**Path Traversal\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=763 |
| Status | New |

Method main at line 115 of freebsd-src-2/maketab.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 115 of freebsd-src-2/maketab.c. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 115 | 132 |
| Object | argv | argv |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
115.  int main(int argc, char *argv[])
....
132.        if ((fp = fopen(argv[1], "r")) == NULL) {
```

## Buffer Overflow AddressOfLocalVarReturned

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

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

*Description*
**Buffer Overflow AddressOfLocalVarReturned\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=37 |
| Status | New |

The pointer d2 at freebsd-src-2/tasn_enc.c in line 373 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/tasn_enc.c | freebsd-src-2/tasn_enc.c |
| Line | 381 | 381 |
| Object | d2 | d2 |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/tasn_enc.c |
| Method | static int der_cmp(const void *a, const void *b) |

```
....
381.      return d1->length - d2->length;
```

**Buffer Overflow AddressOfLocalVarReturned\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=38 |
| Status | New |

The pointer masks at freebsd-src-2/val_nsec.c in line 61 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/val_nsec.c | freebsd-src-2/val_nsec.c |
| Line | 85 | 85 |
| Object | masks | masks |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/val_nsec.c |
| Method | nsecbitmap_has_type_rdata(uint8_t* bitmap, size_t len, uint16_t type) |

```
....
85.               return (int)(bitmap[mybyte] & masks[type_low&0x7]);
```

## 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=1060098&projectid=60088&pathid=1319 |
| Status | New |

The variable declared in null at freebsd-src-2/buffer.c in line 1179 is not initialized when it is used by internal_ at freebsd-src-2/buffer.c in line 1185.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |

| | | |
|---|---|---|
| Line | 1181 | 1203 |
| Object | null | internal_ |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_copyout(struct evbuffer *buf, void *data_out, size_t datlen)

```
....
1181.       return evbuffer_copyout_from(buf, NULL, data_out, datlen);
```

File Name freebsd-src-2/buffer.c

Method evbuffer_copyout_from(struct evbuffer *buf, const struct evbuffer_ptr *pos,

```
....
1203.             pos_in_chain = pos->internal_.pos_in_chain;
```

**NULL Pointer Dereference\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1320 |
| Status | New |

The variable declared in null at freebsd-src-2/buffer.c in line 1165 is not initialized when it is used by internal_ at freebsd-src-2/buffer.c in line 1185.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1169 | 1203 |
| Object | null | internal_ |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_remove(struct evbuffer *buf, void *data_out, size_t datlen)

```
....
1169.       n = evbuffer_copyout_from(buf, NULL, data_out, datlen);
```

File Name freebsd-src-2/buffer.c

Method evbuffer_copyout_from(struct evbuffer *buf, const struct evbuffer_ptr *pos,

```
....
1203.             pos_in_chain = pos->internal_.pos_in_chain;
```

**NULL Pointer Dereference\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1321 |
| Status | New |

The variable declared in null at freebsd-src-2/buffer.c in line 1165 is not initialized when it is used by internal_ at freebsd-src-2/buffer.c in line 1185.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1169 | 1202 |
| Object | null | internal_ |

Code Snippet

File Name freebsd-src-2/buffer.c

Method evbuffer_remove(struct evbuffer *buf, void *data_out, size_t datlen)

```
....
1169.       n = evbuffer_copyout_from(buf, NULL, data_out, datlen);
```

File Name freebsd-src-2/buffer.c

Method evbuffer_copyout_from(struct evbuffer *buf, const struct evbuffer_ptr *pos,

```
....
1202.             chain = pos->internal_.chain;
```

**NULL Pointer Dereference\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1322 |
| Status | New |

The variable declared in null at freebsd-src-2/buffer.c in line 1179 is not initialized when it is used by internal_ at freebsd-src-2/buffer.c in line 1185.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 1181 | 1202 |
| Object | null | internal_ |

Code Snippet

File Name freebsd-src-2/buffer.c

Method evbuffer_copyout(struct evbuffer *buf, void *data_out, size_t datlen)

```
....
1181.       return evbuffer_copyout_from(buf, NULL, data_out, datlen);
```

File Name freebsd-src-2/buffer.c

Method evbuffer_copyout_from(struct evbuffer *buf, const struct evbuffer_ptr *pos,

```
....
1202.             chain = pos->internal_.chain;
```

**NULL Pointer Dereference\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1323 |
| Status | New |

The variable declared in null at freebsd-src-2/buffer.c in line 2702 is not initialized when it is used by internal_ at freebsd-src-2/buffer.c in line 2708.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 2704 | 2727 |
| Object | null | internal_ |

Code Snippet

File Name freebsd-src-2/buffer.c

Method evbuffer_search(struct evbuffer *buffer, const char *what, size_t len, const struct evbuffer_ptr *start)

```
....
2704.       return evbuffer_search_range(buffer, what, len, start,
NULL);
```

File Name freebsd-src-2/buffer.c

Method evbuffer_search_range(struct evbuffer *buffer, const char *what, size_t len, const struct evbuffer_ptr *start, const struct evbuffer_ptr *end)

```
....
2727.             last_chain = end->internal_.chain;
```

**NULL Pointer Dereference\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1324 |
| Status | New |

The variable declared in null at freebsd-src-2/cachedump.c in line 821 is not initialized when it is used by rep at freebsd-src-2/cachedump.c in line 793.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 847 | 799 |
| Object | null | rep |

Code Snippet

File Name freebsd-src-2/cachedump.c

Method int print_deleg_lookup(RES* ssl, struct worker* worker, uint8_t* nm,

```
....
847.              print_dp_main(ssl, dp, NULL);
```

File Name freebsd-src-2/cachedump.c

Method print_dp_main(RES* ssl, struct delegpt* dp, struct dns_msg* msg)

```
....
799.            for(i=0; i<msg->rep->rrset_count; i++) {
```

**NULL Pointer Dereference\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1325 |
| Status | New |

The variable declared in null at freebsd-src-2/cachedump.c in line 821 is not initialized when it is used by rep at freebsd-src-2/cachedump.c in line 793.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 896 | 799 |
| Object | null | rep |

Code Snippet

File Name freebsd-src-2/cachedump.c

Method int print_deleg_lookup(RES* ssl, struct worker* worker, uint8_t* nm,

```
....
896.                    print_dp_main(ssl, stub->dp, NULL);
```

File Name freebsd-src-2/cachedump.c

Method print_dp_main(RES* ssl, struct delegpt* dp, struct dns_msg* msg)

```
....
799.            for(i=0; i<msg->rep->rrset_count; i++) {
```

**NULL Pointer Dereference\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1326 |
| Status | New |

The variable declared in null at freebsd-src-2/ext2_extents.c in line 926 is not initialized when it is used by b_data at freebsd-src-2/ext2_extents.c in line 926.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1005 | 1050 |
| Object | null | b_data |

Code Snippet

File Name freebsd-src-2/ext2_extents.c

Method ext4_ext_split(struct inode *ip, struct ext4_extent_path *path,

```
....
1005.       bp = NULL;
....
1050.             ext2_extent_blk_csum_set(ip, bp->b_data);
```

**NULL Pointer Dereference\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1327 |
| Status | New |

The variable declared in null at freebsd-src-2/ext2_extents.c in line 926 is not initialized when it is used by b_data at freebsd-src-2/ext2_extents.c in line 926.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1052 | 1050 |
| Object | null | b_data |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_split(struct inode *ip, struct ext4_extent_path *path,

```
....
1052.              bp = NULL;
....
1050.              ext2_extent_blk_csum_set(ip, bp->b_data);
```

**NULL Pointer Dereference\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1328 |
| Status | New |

The variable declared in null at freebsd-src-2/ext2_extents.c in line 926 is not initialized when it is used by b_data at freebsd-src-2/ext2_extents.c in line 926.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1005 | 1003 |
| Object | null | b_data |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_ext_split(struct inode *ip, struct ext4_extent_path *path,

```
....
1005.        bp = NULL;
....
1003.        ext2_extent_blk_csum_set(ip, bp->b_data);
```

**NULL Pointer Dereference\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1329 |
| Status | New |

The variable declared in null at freebsd-src-2/if_cpsw.c in line 1610 is not initialized when it is used by bd_offset at freebsd-src-2/if_cpsw.c in line 1610.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/if_cpsw.c | freebsd-src-2/if_cpsw.c |
| Line | 1621 | 1724 |
| Object | null | bd_offset |

Code Snippet
File Name freebsd-src-2/if_cpsw.c
Method cpsw_rx_dequeue(struct cpsw_softc *sc)

```
....
1621.       last = NULL;
....
1724.             cpsw_write_cp_slot(sc, &sc->rx, last);
```

**NULL Pointer Dereference\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1330 |
| Status | New |

The variable declared in null at freebsd-src-2/if_cpsw.c in line 1737 is not initialized when it is used by bd_offset at freebsd-src-2/if_cpsw.c in line 1737.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/if_cpsw.c | freebsd-src-2/if_cpsw.c |
| Line | 1745 | 1804 |
| Object | null | bd_offset |

Code Snippet
File Name freebsd-src-2/if_cpsw.c
Method cpsw_rx_enqueue(struct cpsw_softc *sc)

```
....
1745.       first_new_slot = NULL;
....
1804.             cpsw_write_hdp_slot(sc, &sc->rx, first_new_slot);
```

**NULL Pointer Dereference\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1331 |
| Status | New |

The variable declared in null at freebsd-src-2/if_cpsw.c in line 1737 is not initialized when it is used by bd_offset at freebsd-src-2/if_cpsw.c in line 1737.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/if_cpsw.c | freebsd-src-2/if_cpsw.c |
| Line | 1745 | 1807 |
| Object | null | bd_offset |

Code Snippet
File Name freebsd-src-2/if_cpsw.c
Method cpsw_rx_enqueue(struct cpsw_softc *sc)

```
....
1745.        first_new_slot = NULL;
....
1807.              cpsw_cpdma_write_bd_next(sc, last_old_slot,
first_new_slot);
```

**NULL Pointer Dereference\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1332 |
| Status | New |

The variable declared in null at freebsd-src-2/if_cpsw.c in line 1848 is not initialized when it is used by bd_offset at freebsd-src-2/if_cpsw.c in line 1848.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/if_cpsw.c | freebsd-src-2/if_cpsw.c |
| Line | 1858 | 1978 |
| Object | null | bd_offset |

Code Snippet
File Name freebsd-src-2/if_cpsw.c
Method cpswp_tx_enqueue(struct cpswp_softc *sc)

```
....
1858.        first_new_slot = NULL;
....
1978.              cpsw_cpdma_write_bd_next(sc->swsc, last_old_slot,
```

**NULL Pointer Dereference\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1333 |
| Status | New |

The variable declared in null at freebsd-src-2/if_cpsw.c in line 1848 is not initialized when it is used by bd_offset at freebsd-src-2/if_cpsw.c in line 1848.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/if_cpsw.c | freebsd-src-2/if_cpsw.c |
| Line | 1858 | 1982 |
| Object | null | bd_offset |

Code Snippet
File Name freebsd-src-2/if_cpsw.c
Method cpswp_tx_enqueue(struct cpswp_softc *sc)

```
....
1858.       first_new_slot = NULL;
....
1982.             cpsw_write_hdp_slot(sc->swsc, &sc->swsc->tx,
first_new_slot);
```

**NULL Pointer Dereference\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1334 |
| Status | New |

The variable declared in null at freebsd-src-2/ip6_output.c in line 409 is not initialized when it is used by ia_ifa at freebsd-src-2/ip6_output.c in line 409.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 425 | 1267 |
| Object | null | ia_ifa |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_output(struct mbuf *m0, struct ip6_pktopts *opt,

```
....
425.        struct in6_ifaddr *ia = NULL;
....
1267.                          counter_u64_add(ia->ia_ifa.ifa_obytes,
```

**NULL Pointer Dereference\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1335 |
| Status | New |

The variable declared in null at freebsd-src-2/ip6_output.c in line 409 is not initialized when it is used by ia_ifa at freebsd-src-2/ip6_output.c in line 409.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 425 | 1266 |

| | | |
|---|---|---|
| Object | null | ia_ifa |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_output(struct mbuf *m0, struct ip6_pktopts *opt,

```
....
425.        struct in6_ifaddr *ia = NULL;
....
1266.                           counter_u64_add(ia->ia_ifa.ifa_opackets,
1);
```

**NULL Pointer Dereference\Path 18:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1336
Status New

The variable declared in null at freebsd-src-2/ip6_output.c in line 409 is not initialized when it is used by nh_pksent at freebsd-src-2/ip6_output.c in line 409.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 673 | 729 |
| Object | null | nh_pksent |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_output(struct mbuf *m0, struct ip6_pktopts *opt,

```
....
673.        nh = NULL;
....
729.                    counter_u64_add(nh->nh_pksent, 1);
```

**NULL Pointer Dereference\Path 19:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1337
Status New

The variable declared in null at freebsd-src-2/krb5_mech.c in line 1399 is not initialized when it is used by m_len at freebsd-src-2/krb5_mech.c in line 1399.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |

| | | |
|---|---|---|
| Line | 1448 | 1532 |
| Object | null | m_len |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1448.                    tm = NULL;
....
1532.              tm->m_len -= 16;
```

**NULL Pointer Dereference\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1338 |
| Status | New |

The variable declared in null at freebsd-src-2/krb5_mech.c in line 1399 is not initialized when it is used by m_data at freebsd-src-2/krb5_mech.c in line 1399.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1448 | 1529 |
| Object | null | m_data |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1448.                    tm = NULL;
....
1529.              bcopy(p, tm->m_data, 16);
```

**NULL Pointer Dereference\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1339 |
| Status | New |

The variable declared in null at freebsd-src-2/krb5_mech.c in line 1399 is not initialized when it is used by m_data at freebsd-src-2/krb5_mech.c in line 1399.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1448 | 1531 |
| Object | null | m_data |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1448.                    tm = NULL;
....
1531.              tm->m_data += 16;
```

**NULL Pointer Dereference\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1340 |
| Status | New |

The variable declared in null at freebsd-src-2/print-openflow.c in line 144 is not initialized when it is used by mti at freebsd-src-2/print-openflow.c in line 107.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-openflow.c | freebsd-src-2/print-openflow.c |
| Line | 167 | 132 |
| Object | null | mti |

Code Snippet
File Name freebsd-src-2/print-openflow.c
Method openflow_print(netdissect_options *ndo, const u_char *cp, u_int len)

```
....
167.                    NULL;
```

File Name freebsd-src-2/print-openflow.c
Method of_message_print(netdissect_options *ndo,

```
....
132.        mti->decoder(ndo, cp, len);
```

**NULL Pointer Dereference\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1341 |
| Status | New |

The variable declared in null at freebsd-src-2/print-openflow.c in line 144 is not initialized when it is used by decoder at freebsd-src-2/print-openflow.c in line 107.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-openflow.c | freebsd-src-2/print-openflow.c |
| Line | 167 | 129 |
| Object | null | decoder |

Code Snippet

File Name freebsd-src-2/print-openflow.c

Method openflow_print(netdissect_options *ndo, const u_char *cp, u_int len)

```
....
167.                    NULL;
```

File Name freebsd-src-2/print-openflow.c

Method of_message_print(netdissect_options *ndo,

```
....
129.        if (!ndo->ndo_vflag || !mti->decoder)
```

**NULL Pointer Dereference\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1342 |
| Status | New |

The variable declared in null at freebsd-src-2/rtsol.c in line 159 is not initialized when it is used by ipi6_ifindex at freebsd-src-2/rtsol.c in line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 169 | 245 |
| Object | null | ipi6_ifindex |

Code Snippet

File Name freebsd-src-2/rtsol.c

Method rtsol_input(int sock)

```
....
169.        struct in6_pktinfo *pi = NULL;
....
245.                    if_indextoname(pi->ipi6_ifindex, ifnamebuf));
```

**NULL Pointer Dereference\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1343 |
| Status | New |

The variable declared in null at freebsd-src-2/rtsol.c in line 159 is not initialized when it is used by ipi6_ifindex at freebsd-src-2/rtsol.c in line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 169 | 254 |
| Object | null | ipi6_ifindex |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
169.        struct in6_pktinfo *pi = NULL;
....
254.                    if_indextoname(pi->ipi6_ifindex, ifnamebuf));
```

**NULL Pointer Dereference\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1344 |
| Status | New |

The variable declared in null at freebsd-src-2/rtsol.c in line 159 is not initialized when it is used by ipi6_ifindex at freebsd-src-2/rtsol.c in line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 169 | 264 |
| Object | null | ipi6_ifindex |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method rtsol_input(int sock)

```
....
169.        struct in6_pktinfo *pi = NULL;
....
264.                    if_indextoname(pi->ipi6_ifindex, ifnamebuf));
```

**NULL Pointer Dereference\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1345 |
| Status | New |

The variable declared in null at freebsd-src-2/server.c in line 154 is not initialized when it is used by l2cap_bdaddr at freebsd-src-2/server.c in line 154.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/server.c | freebsd-src-2/server.c |
| Line | 240 | 252 |
| Object | null | l2cap_bdaddr |

Code Snippet
File Name freebsd-src-2/server.c
Method server_read(int s, short ev, void *arg)

```
....
240.        log_info("Accepted connection from %s",
bt_ntoa(&ra.l2cap_bdaddr, NULL));
....
252.        b2eaddr(chan->raddr, &ra.l2cap_bdaddr);
```

**NULL Pointer Dereference\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1346 |
| Status | New |

The variable declared in null at freebsd-src-2/statem_dtls.c in line 467 is not initialized when it is used by msg_header at freebsd-src-2/statem_dtls.c in line 467.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 492 | 511 |
| Object | null | msg_header |

Code Snippet
File Name freebsd-src-2/statem_dtls.c

Method static int dtls1_retrieve_buffered_fragment(SSL *s, size_t *len)

```
....
492.                frag = NULL;
....
511.                        frag->msg_header.frag_len);
```

**NULL Pointer Dereference\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1347 |
| Status | New |

The variable declared in null at freebsd-src-2/statem_dtls.c in line 467 is not initialized when it is used by msg_header at freebsd-src-2/statem_dtls.c in line 467.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 492 | 510 |
| Object | null | msg_header |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method static int dtls1_retrieve_buffered_fragment(SSL *s, size_t *len)

```
....
492.                frag = NULL;
....
510.                memcpy(&p[frag->msg_header.frag_off], frag->fragment,
```

**NULL Pointer Dereference\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1348 |
| Status | New |

The variable declared in null at freebsd-src-2/statem_dtls.c in line 467 is not initialized when it is used by msg_header at freebsd-src-2/statem_dtls.c in line 467.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 492 | 507 |
| Object | null | msg_header |

Code Snippet
File Name freebsd-src-2/statem_dtls.c

Method static int dtls1_retrieve_buffered_fragment(SSL *s, size_t *len)

```
....
492.                frag = NULL;
....
507.            if (ret && frag->msg_header.frag_len > 0) {
```

**NULL Pointer Dereference\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1349 |
| Status | New |

The variable declared in null at freebsd-src-2/statem_dtls.c in line 467 is not initialized when it is used by msg_header at freebsd-src-2/statem_dtls.c in line 467.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 492 | 501 |
| Object | null | msg_header |

Code Snippet
File Name freebsd-src-2/statem_dtls.c
Method static int dtls1_retrieve_buffered_fragment(SSL *s, size_t *len)

```
....
492.                frag = NULL;
....
501.            size_t frag_len = frag->msg_header.frag_len;
```

**NULL Pointer Dereference\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1350 |
| Status | New |

The variable declared in null at freebsd-src-2/statem_dtls.c in line 467 is not initialized when it is used by msg_header at freebsd-src-2/statem_dtls.c in line 467.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 492 | 500 |
| Object | null | msg_header |

Code Snippet
File Name freebsd-src-2/statem_dtls.c

| | |
|---|---|
| Method | static int dtls1_retrieve_buffered_fragment(SSL *s, size_t *len) |

```
....
492.                frag = NULL;
....
500.        if (s->d1->handshake_read_seq == frag->msg_header.seq) {
```

**NULL Pointer Dereference\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1351 |
| Status | New |

The variable declared in null at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by reassembly at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 565 | 609 |
| Object | null | reassembly |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/statem_dtls.c |
| Method | dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr) |

```
....
565.                frag = NULL;
....
609.            OPENSSL_free(frag->reassembly);
```

**NULL Pointer Dereference\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1352 |
| Status | New |

The variable declared in null at freebsd-src-2/statem_dtls.c in line 531 is not initialized when it is used by reassembly at freebsd-src-2/statem_dtls.c in line 531.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_dtls.c | freebsd-src-2/statem_dtls.c |
| Line | 565 | 575 |
| Object | null | reassembly |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/statem_dtls.c |

| | |
|---|---|
| Method | dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr) |

```
....
565.                frag = NULL;
....
575.        if (frag->reassembly == NULL) {
```

**NULL Pointer Dereference\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1353 |
| Status | New |

The variable declared in null at freebsd-src-2/vnic_dev.c in line 929 is not initialized when it is used by res at freebsd-src-2/vnic_dev.c in line 36.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vnic_dev.c | freebsd-src-2/vnic_dev.c |
| Line | 932 | 107 |
| Object | null | res |

Code Snippet

File Name freebsd-src-2/vnic_dev.c

Method struct vnic_dev *vnic_dev_register(struct vnic_dev *vdev,

```
....
932.        if (vnic_dev_discover_res(vdev, NULL, num_bars))
```

File Name freebsd-src-2/vnic_dev.c

Method static int vnic_dev_discover_res(struct vnic_dev *vdev,

```
....
107.                bcopy(&softc->mem, &vdev->res[type].bar, sizeof(softc->mem));
```

**NULL Pointer Dereference\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1354 |
| Status | New |

The variable declared in 0 at freebsd-src-2/buffer.c in line 670 is not initialized when it is used by iov_len at freebsd-src-2/buffer.c in line 670.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 686 | 686 |
| Object | 0 | iov_len |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_reserve_space(struct evbuffer *buf, ev_ssize_t size,

```
....
686.                vec[0].iov_len = (size_t)CHAIN_SPACE_LEN(chain);
```

**NULL Pointer Dereference\Path 37:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1355
Status New

The variable declared in 0 at freebsd-src-2/print-udp.c in line 215 is not initialized when it is used by rr_dv at freebsd-src-2/print-udp.c in line 215.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-udp.c | freebsd-src-2/print-udp.c |
| Line | 218 | 289 |
| Object | 0 | rr_dv |

Code Snippet
File Name freebsd-src-2/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
218.        const struct rtcp_rr *rr = 0;
....
289.                    GET_BE_U_4(rr->rr_dv), ts, dts);
```

**NULL Pointer Dereference\Path 38:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1356
Status New

The variable declared in 0 at freebsd-src-2/print-udp.c in line 215 is not initialized when it is used by rr_ls at freebsd-src-2/print-udp.c in line 215.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-udp.c | freebsd-src-2/print-udp.c |

| | | |
|---|---|---|
| Line | 218 | 288 |
| Object | 0 | rr_ls |

Code Snippet
File Name freebsd-src-2/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
218.        const struct rtcp_rr *rr = 0;
....
288.                    GET_BE_U_4(rr->rr_ls),
```

**NULL Pointer Dereference\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1357 |
| Status | New |

The variable declared in 0 at freebsd-src-2/print-udp.c in line 215 is not initialized when it is used by rr_nl at freebsd-src-2/print-udp.c in line 215.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-udp.c | freebsd-src-2/print-udp.c |
| Line | 218 | 287 |
| Object | 0 | rr_nl |

Code Snippet
File Name freebsd-src-2/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
218.        const struct rtcp_rr *rr = 0;
....
287.                    GET_BE_U_4(rr->rr_nl) & 0x00ffffff,
```

**NULL Pointer Dereference\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1358 |
| Status | New |

The variable declared in 0 at freebsd-src-2/print-udp.c in line 215 is not initialized when it is used by rr_srcid at freebsd-src-2/print-udp.c in line 215.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/print-udp.c | freebsd-src-2/print-udp.c |
| Line | 218 | 283 |
| Object | 0 | rr_srcid |

Code Snippet
File Name freebsd-src-2/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
218.        const struct rtcp_rr *rr = 0;
....
283.                    ND_PRINT(" %u", GET_BE_U_4(rr->rr_srcid));
```

**NULL Pointer Dereference\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1359 |
| Status | New |

The variable declared in 0 at freebsd-src-2/rt2860.c in line 1455 is not initialized when it is used by xflags at freebsd-src-2/rt2860.c in line 1455.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 1521 | 1521 |
| Object | 0 | xflags |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_tx(struct rt2860_softc *sc, struct mbuf *m, struct ieee80211_node *ni)

```
....
1521.       txwi->xflags = qos ? 0 : RT2860_TX_NSEQ;
```

**NULL Pointer Dereference\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1360 |
| Status | New |

The variable declared in 0 at freebsd-src-2/rt2860.c in line 1455 is not initialized when it is used by xflags at freebsd-src-2/rt2860.c in line 1455.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |

| | | |
|---|---|---|
| Line | 1521 | 1558 |
| Object | 0 | xflags |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_tx(struct rt2860_softc *sc, struct mbuf *m, struct ieee80211_node *ni)

```
....
1521.       txwi->xflags = qos ? 0 : RT2860_TX_NSEQ;
....
1558.             txwi->xflags |= RT2860_TX_ACK;
```

**NULL Pointer Dereference\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1361
Status New

The variable declared in 0 at freebsd-src-2/rt2860.c in line 1728 is not initialized when it is used by xflags at freebsd-src-2/rt2860.c in line 1728.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 1772 | 1772 |
| Object | 0 | xflags |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_tx_raw(struct rt2860_softc *sc, struct mbuf *m,

```
....
1772.       txwi->xflags = params->ibp_pri & 3 ? 0 : RT2860_TX_NSEQ;
```

**NULL Pointer Dereference\Path 44:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1362
Status New

The variable declared in 0 at freebsd-src-2/rt2860.c in line 1728 is not initialized when it is used by xflags at freebsd-src-2/rt2860.c in line 1728.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 1772 | 1801 |

| | | |
|---|---|---|
| Object | 0 | xflags |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_tx_raw(struct rt2860_softc *sc, struct mbuf *m,

```
....
1772.       txwi->xflags = params->ibp_pri & 3 ? 0 : RT2860_TX_NSEQ;
....
1801.             txwi->xflags |= RT2860_TX_ACK;
```

**NULL Pointer Dereference\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1363
Status New

The variable declared in 0 at freebsd-src-2/rt2860.c in line 3353 is not initialized when it is used by freq at freebsd-src-2/rt2860.c in line 3353.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 3412 | 3412 |
| Object | 0 | freq |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_read_eeprom(struct rt2860_softc *sc, uint8_t macaddr[IEEE80211_ADDR_LEN])

```
....
3412.       sc->freq = ((val & 0xff) != 0xff) ? val & 0xff : 0;
```

**NULL Pointer Dereference\Path 46:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1364
Status New

The variable declared in 0 at freebsd-src-2/server.c in line 265 is not initialized when it is used by security_description at freebsd-src-2/server.c in line 265.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/server.c | freebsd-src-2/server.c |
| Line | 281 | 281 |

| | | |
|---|---|---|
| Object | 0 | security_description |

Code Snippet
File Name freebsd-src-2/server.c
Method server_register(void)

```
....
281.        p.security_description = (l2cap_mode == 0 ? 0x0000 :
0x0001);
```

**NULL Pointer Dereference\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1365 |
| Status | New |

The variable declared in 0 at freebsd-src-2/valectl.c in line 85 is not initialized when it is used by Pointer at freebsd-src-2/valectl.c in line 85.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 94 | 120 |
| Object | 0 | Pointer |

Code Snippet
File Name freebsd-src-2/valectl.c
Method parse_ring_config(const char* conf,

```
....
94.    *nr_tx_rings = *nr_rx_rings = 0;
....
120.                    *nr_tx_rings, *nr_tx_slots,
```

**NULL Pointer Dereference\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1366 |
| Status | New |

The variable declared in 0 at freebsd-src-2/valectl.c in line 85 is not initialized when it is used by Pointer at freebsd-src-2/valectl.c in line 85.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 94 | 121 |

| | | |
|---|---|---|
| Object | 0 | Pointer |

Code Snippet
File Name freebsd-src-2/valectl.c
Method parse_ring_config(const char* conf,

```
....
94.    *nr_tx_rings = *nr_rx_rings = 0;
....
121.                       *nr_rx_rings, *nr_rx_slots);
```

**NULL Pointer Dereference\Path 49:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1367
Status New

The variable declared in 0 at freebsd-src-2/valectl.c in line 85 is not initialized when it is used by Pointer at freebsd-src-2/valectl.c in line 85.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 95 | 120 |
| Object | 0 | Pointer |

Code Snippet
File Name freebsd-src-2/valectl.c
Method parse_ring_config(const char* conf,

```
....
95.    *nr_tx_slots = *nr_rx_slots = 0;
....
120.                       *nr_tx_rings, *nr_tx_slots,
```

**NULL Pointer Dereference\Path 50:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1368
Status New

The variable declared in 0 at freebsd-src-2/valectl.c in line 85 is not initialized when it is used by Pointer at freebsd-src-2/valectl.c in line 85.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |

| | | |
|---|---|---|
| Line | 95 | 121 |
| Object | 0 | Pointer |

Code Snippet
File Name freebsd-src-2/valectl.c
Method parse_ring_config(const char* conf,

```
....
95.    *nr_tx_slots = *nr_rx_slots = 0;
....
121.                     *nr_rx_rings, *nr_rx_slots);
```

## 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=1060098&projectid=60088&pathid=931 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 138 | 138 |
| Object | fgets | fgets |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
138.        while (fgets(buf, sizeof buf, fp) != NULL) {
```

**Improper Resource Access Authorization\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=932 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 803 | 803 |
| Object | fgets | fgets |

Code Snippet
File Name freebsd-src-2/session.c
Method do_motd(void)

```
....
803.                    while (fgets(buf, sizeof(buf), f))
```

**Improper Resource Access Authorization\Path 3:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=933
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1313 | 1313 |
| Object | fgets | fgets |

Code Snippet
File Name freebsd-src-2/session.c
Method do_nologin(struct passwd *pw)

```
....
1313.             while (fgets(buf, sizeof(buf), f))
```

**Improper Resource Access Authorization\Path 4:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=934
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3173 | 3173 |
| Object | fgets | fgets |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/test_main.c |
| Method | extract_reference_file(const char *name) |

```
....
3173.             if (fgets(buff, sizeof(buff), in) == NULL) {
```

**Improper Resource Access Authorization\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=935 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3182 | 3182 |
| Object | fgets | fgets |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/test_main.c |
| Method | extract_reference_file(const char *name) |

```
....
3182.       while (fgets(buff, sizeof(buff), in) != NULL) {
```

**Improper Resource Access Authorization\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=936 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/gethostid.c | freebsd-src-2/gethostid.c |
| Line | 50 | 50 |
| Object | fscanf | fscanf |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/gethostid.c |
| Method | get_spl_hostid(void) |

```
....
50.   if (fscanf(f, "%lx", &hostid) != 1)
```

**Improper Resource Access Authorization\Path 7:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=937 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 138 | 138 |
| Object | buf | buf |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
138.        while (fgets(buf, sizeof buf, fp) != NULL) {
```

**Improper Resource Access Authorization\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=938 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 803 | 803 |
| Object | buf | buf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_motd(void)

```
....
803.                    while (fgets(buf, sizeof(buf), f))
```

**Improper Resource Access Authorization\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=939 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |

| | | |
|---|---|---|
| Line | 1313 | 1313 |
| Object | buf | buf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_nologin(struct passwd *pw)

```
....
1313.             while (fgets(buf, sizeof(buf), f))
```

**Improper Resource Access Authorization\Path 10:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=940
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3173 | 3173 |
| Object | buff | buff |

Code Snippet
File Name freebsd-src-2/test_main.c
Method extract_reference_file(const char *name)

```
....
3173.             if (fgets(buff, sizeof(buff), in) == NULL) {
```

**Improper Resource Access Authorization\Path 11:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=941
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3182 | 3182 |
| Object | buff | buff |

Code Snippet
File Name freebsd-src-2/test_main.c
Method extract_reference_file(const char *name)

```
....
3182.       while (fgets(buff, sizeof(buff), in) != NULL) {
```

**Improper Resource Access Authorization\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=942 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 992 | 992 |
| Object | buff | buff |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_empty_file(const char *filename, int line, const char *f1)

```
....
992.              s = fread(buff, 1, s, f);
```

**Improper Resource Access Authorization\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=943 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1041 | 1041 |
| Object | buff1 | buff1 |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_equal_file(const char *filename, int line, const char *fn1, const char *fn2)

```
....
1041.             n1 = (int)fread(buff1, 1, sizeof(buff1), f1);
```

**Improper Resource Access Authorization\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=944 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1042 | 1042 |
| Object | buff2 | buff2 |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_equal_file(const char *filename, int line, const char *fn1, const char *fn2)

```
....
1042.             n2 = (int)fread(buff2, 1, sizeof(buff2), f2);
```

**Improper Resource Access Authorization\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=945 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1116 | 1116 |
| Object | contents | contents |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_contents(const char *filename, int line, const void *buff, int s, const char *fn)

```
....
1116.       n = (int)fread(contents, 1, s * 2, f);
```

**Improper Resource Access Authorization\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=946 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1154 | 1154 |
| Object | contents | contents |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_text_file_contents(const char *filename, int line, const char *buff, const char *fn)

```
....
1154.       n = (int)fread(contents, 1, s * 2 + 128 - 1, f);
```

**Improper Resource Access Authorization\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=947
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3119 | 3119 |
| Object | p | p |

Code Snippet
File Name freebsd-src-2/test_main.c
Method slurpfile(size_t * sizep, const char *fmt, ...)

```
....
3119.       bytes_read = fread(p, 1, (size_t)st.st_size, f);
```

**Improper Resource Access Authorization\Path 18:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=948
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3233 | 3233 |
| Object | buff | buff |

Code Snippet
File Name freebsd-src-2/test_main.c

| | |
|---|---|
| Method | copy_reference_file(const char *name) |

```
....
3233.       while ((rbytes = fread(buff, 1, sizeof(buff), in)) > 0) {
```

**Improper Resource Access Authorization\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=949 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/gethostid.c | freebsd-src-2/gethostid.c |
| Line | 50 | 50 |
| Object | Address | Address |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/gethostid.c |
| Method | get_spl_hostid(void) |

```
....
50.   if (fscanf(f, "%lx", &hostid) != 1)
```

**Improper Resource Access Authorization\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=950 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 3107 | 3107 |
| Object | BinaryExpr | BinaryExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_file_segment_materialize(struct evbuffer_file_segment *seg) |

```
....
3107.                   n = read(fd, mem+read_so_far, length-
read_so_far);
```

**Improper Resource Access Authorization\Path 21:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=951 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/dtstream.c | freebsd-src-2/dtstream.c |
| Line | 1549 | 1549 |
| Object | Address | Address |

Code Snippet
File Name freebsd-src-2/dtstream.c
Method void dtio_cmd_cb(int fd, short ATTR_UNUSED(bits), void* arg)

```
....
1549.        r = read(fd, &cmd, sizeof(cmd));
```

**Improper Resource Access Authorization\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=952 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/gethostid.c | freebsd-src-2/gethostid.c |
| Line | 73 | 73 |
| Object | Address | Address |

Code Snippet
File Name freebsd-src-2/gethostid.c
Method get_system_hostid(void)

```
....
73.                if (read(fd, &system_hostid, sizeof (system_hostid))
```

**Improper Resource Access Authorization\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=953 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cut.c | freebsd-src-2/cut.c |

| | | |
|---|---|---|
| Line | 482 | 482 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/cut.c
Method usage(void)

```
....
482.         (void)fprintf(stderr, "%s\n%s\n%s\n",
```

**Improper Resource Access Authorization\Path 24:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=954
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/diff.c | freebsd-src-2/diff.c |
| Line | 587 | 587 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/diff.c
Method usage(void)

```
....
587.         (void)fprintf(help ? stdout : stderr,
```

**Improper Resource Access Authorization\Path 25:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=955
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/diff.c | freebsd-src-2/diff.c |
| Line | 619 | 619 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/diff.c
Method conflicting_format(void)

```
....
619.        fprintf(stderr, "error: conflicting output format
options.\n");
```

**Improper Resource Access Authorization\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=956 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 351 | 351 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/http-server.c
Method main(int argc, char **argv)

```
....
351.              fprintf(stderr, "Couldn't create an event_base:
exiting\n");
```

**Improper Resource Access Authorization\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=957 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 358 | 358 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/http-server.c
Method main(int argc, char **argv)

```
....
358.              fprintf(stderr, "couldn't create evhttp. Exiting.\n");
```

**Improper Resource Access Authorization\Path 28:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=958 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 372 | 372 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/http-server.c
Method main(int argc, char **argv)

```
....
372.                fprintf(stderr, "couldn't bind to port %d.
Exiting.\n",
```

**Improper Resource Access Authorization\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=959 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 399 | 399 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/http-server.c
Method main(int argc, char **argv)

```
....
399.                    fprintf(stderr, "Weird address family %d\n",
```

**Improper Resource Access Authorization\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=960 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 410 | 410 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/http-server.c
Method main(int argc, char **argv)

```
....
410.                    fprintf(stderr, "evutil_inet_ntop failed\n");
```

**Improper Resource Access Authorization\Path 31:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=961
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 326 | 326 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/http-server.c
Method syntax(void)

```
....
326.        fprintf(stdout, "Syntax: http-server <docroot>\n");
```

**Improper Resource Access Authorization\Path 32:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=962
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 86 | 86 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method usage(char *name)

```
....
86.   fprintf(stderr, "Usage: %s [-CFhlnrRsv] [-f filename]\n", name);
```

**Improper Resource Access Authorization\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=963 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 169 | 169 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method main(int argc, char *argv[])

```
....
169.              (void) fprintf(stderr, "%s: -p must be used with -
r\n",
```

**Improper Resource Access Authorization\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=964 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 184 | 184 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method main(int argc, char *argv[])

```
....
184.                    (void) fprintf(stderr, "%s: open: %s\n",
IPNAT_NAME,
```

**Improper Resource Access Authorization\Path 35:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=965 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 194 | 194 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method main(int argc, char *argv[])

```
....
194.                    fprintf(stderr, "User/kernel version check
failed\n");
```

**Improper Resource Access Authorization\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=966 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 253 | 253 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method natstat_dead(natstat_t *nsp, char *kernel)

```
....
253.              fprintf(stderr, "nlist error\n");
```

**Improper Resource Access Authorization\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=967 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 406 | 406 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method dotable(natstat_t *nsp, int fd, int alive, int which, char *side)

```
....
406.                fprintf(stderr,
```

**Improper Resource Access Authorization\Path 38:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=968
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 129 | 129 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
129.                fprintf(stderr, "usage: maketab YTAB_H\n");
```

**Improper Resource Access Authorization\Path 39:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=969
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 133 | 133 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
133.              fprintf(stderr, "maketab can't open %s!\n", argv[1]);
```

**Improper Resource Access Authorization\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=970 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 167 | 167 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
167.                    fprintf(stderr, "maketab out of space copying
%s", name);
```

**Improper Resource Access Authorization\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=971 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/mem_dbg.c | freebsd-src-2/mem_dbg.c |
| Line | 561 | 561 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/mem_dbg.c
Method static void print_leak(const MEM *m, MEM_LEAK *l)

```
....
561.              fprintf(stderr, "##> %s\n", strings[i]);
```

**Improper Resource Access Authorization\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=972 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/parsenfsfh.c | freebsd-src-2/parsenfsfh.c |
| Line | 400 | 400 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/parsenfsfh.c
Method Parse_fh(netdissect_options *ndo, const unsigned char *fh, u_int len,

```
....
400.                (void)fprintf(stderr, "%x.", GET_U_1(fhp + i));
```

**Improper Resource Access Authorization\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=973 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/parsenfsfh.c | freebsd-src-2/parsenfsfh.c |
| Line | 401 | 401 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/parsenfsfh.c
Method Parse_fh(netdissect_options *ndo, const unsigned char *fh, u_int len,

```
....
401.                (void)fprintf(stderr, "\n");
```

**Improper Resource Access Authorization\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=974 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |

| | | |
|---|---|---|
| Line | 241 | 241 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_local_cmd(arglist *a)

```
....
241.              fprintf(stderr, "Executing:");
```

**Improper Resource Access Authorization\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=975
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 244 | 244 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_local_cmd(arglist *a)

```
....
244.              fprintf(stderr, "\n");
```

**Improper Resource Access Authorization\Path 46:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=976
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 743 | 743 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_times(int fd, int verb, const struct stat *sb)

```
....
743.              fprintf(stderr, "File mtime %lld atime %lld\n",
```

**Improper Resource Access Authorization\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=977 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 745 | 745 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_times(int fd, int verb, const struct stat *sb)

```
....
745.              fprintf(stderr, "Sending file timestamps: %s", buf);
```

**Improper Resource Access Authorization\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=978 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 2097 | 2097 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method usage(void)

```
....
2097.       (void) fprintf(stderr,
```

**Improper Resource Access Authorization\Path 49:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=979 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 2112 | 2112 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method run_err(const char *fmt,...)

```
....
2112.             (void) fprintf(fp, "%c", 0x01);
```

**Improper Resource Access Authorization\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=980 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 2113 | 2113 |
| Object | fprintf | fprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method run_err(const char *fmt,...)

```
....
2113.             (void) fprintf(fp, "scp: ");
```

## 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=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1164 |
| Status | New |

The acpi_tz_attach method calls the snprintf function, at line 201 of freebsd-src-2/acpi_thermal.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-2/acpi_thermal.c | freebsd-src-2/acpi_thermal.c |
| Line | 262 | 262 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/acpi_thermal.c
Method acpi_tz_attach(device_t dev)

```
....
262.      snprintf(oidname, sizeof(oidname), "tz%d",
device_get_unit(dev));
```

**Unchecked Return Value\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1165 |
| Status | New |

The acpi_tz_establish method calls the sprintf function, at line 386 of freebsd-src-2/acpi_thermal.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-2/acpi_thermal.c | freebsd-src-2/acpi_thermal.c |
| Line | 411 | 411 |
| Object | sprintf | sprintf |

Code Snippet
File Name freebsd-src-2/acpi_thermal.c
Method acpi_tz_establish(struct acpi_tz_softc *sc)

```
....
411.          sprintf(nbuf, "_AC%d", i);
```

**Unchecked Return Value\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1166 |
| Status | New |

The acpi_tz_establish method calls the sprintf function, at line 386 of freebsd-src-2/acpi_thermal.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-2/acpi_thermal.c | freebsd-src-2/acpi_thermal.c |
| Line | 413 | 413 |
| Object | sprintf | sprintf |

Code Snippet
File Name freebsd-src-2/acpi_thermal.c
Method acpi_tz_establish(struct acpi_tz_softc *sc)

```
....
413.        sprintf(nbuf, "_AL%d", i);
```

**Unchecked Return Value\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1167 |
| Status | New |

The fwe_ioctl method calls the snprintf function, at line 353 of freebsd-src-2/if_fwe.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-2/if_fwe.c | freebsd-src-2/if_fwe.c |
| Line | 380 | 380 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/if_fwe.c
Method fwe_ioctl(if_t ifp, u_long cmd, caddr_t data)

```
....
380.                    snprintf(ifs->ascii, sizeof(ifs->ascii),
```

**Unchecked Return Value\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1168 |

| Status | New |
|---|---|

The mt7615_thermal_show_temp method calls the sprintf function, at line 18 of freebsd-src-2/init.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-2/init.c | freebsd-src-2/init.c |
| Line | 36 | 36 |
| Object | sprintf | sprintf |

Code Snippet
File Name freebsd-src-2/init.c
Method static ssize_t mt7615_thermal_show_temp(struct device *dev,

```
....
36.    return sprintf(buf, "%u\n", temperature * 1000);
```

**Unchecked Return Value\Path 6:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1169 |
| Status | New |

The Parse_fh method calls the snprintf function, at line 85 of freebsd-src-2/parsenfsfh.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-2/parsenfsfh.c | freebsd-src-2/parsenfsfh.c |
| Line | 405 | 405 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/parsenfsfh.c
Method Parse_fh(netdissect_options *ndo, const unsigned char *fh, u_int len,

```
....
405.                (void)snprintf(&(fsidp->Opaque_Handle[i*2]), 3,
"%.2X",
```

**Unchecked Return Value\Path 7:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1170 |

| Status | New |
|---|---|

The isis_print_id method calls the snprintf function, at line 1752 of freebsd-src-2/print-isoclns.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-2/print-isoclns.c | freebsd-src-2/print-isoclns.c |
| Line | 1763 | 1763 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-isoclns.c
Method isis_print_id(netdissect_options *ndo, const uint8_t *cp, u_int id_len)

```
....
1763.           snprintf(pos, sizeof(id) - (pos - id), "%02x",
GET_U_1(cp));
```

**Unchecked Return Value\Path 8:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1171 |
| Status | New |

The isis_print_id method calls the snprintf function, at line 1752 of freebsd-src-2/print-isoclns.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-2/print-isoclns.c | freebsd-src-2/print-isoclns.c |
| Line | 1770 | 1770 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-isoclns.c
Method isis_print_id(netdissect_options *ndo, const uint8_t *cp, u_int id_len)

```
....
1770.           snprintf(pos, sizeof(id) - (pos - id), ".%02x",
GET_U_1(cp));
```

**Unchecked Return Value\Path 9:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1172 |
| Status | New |

The isis_print_id method calls the snprintf function, at line 1752 of freebsd-src-2/print-isocln s.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-2/print-isocln s.c | freebsd-src-2/print-isocln s.c |
| Line | 1775 | 1775 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-isocln s.c
Method isis_print_id(netdissect_options *ndo, const uint8_t *cp, u_int id_len)

```
....
1775.           snprintf(pos, sizeof(id) - (pos - id), "-%02x",
GET_U_1(cp));
```

**Unchecked Return Value\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1173 |
| Status | New |

The isis_print_ext_is_reach method calls the snprintf function, at line 1950 of freebsd-src-2/print-isocln s.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-2/print-isocln s.c | freebsd-src-2/print-isocln s.c |
| Line | 1993 | 1993 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-isocln s.c
Method isis_print_ext_is_reach(netdissect_options *ndo,

```
....
1993.           snprintf(ident_buffer, sizeof(ident_buffer), "%s
",ident);
```

**Unchecked Return Value\Path 11:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1174 |
| Status | New |

The isis_print_extd_ip_reach method calls the snprintf function, at line 2272 of freebsd-src-2/print-isoclns.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-2/print-isoclns.c | freebsd-src-2/print-isoclns.c |
| Line | 2354 | 2354 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-isoclns.c
Method isis_print_extd_ip_reach(netdissect_options *ndo,

```
....
2354.                snprintf(ident_buffer, sizeof(ident_buffer), "%s
",ident);
```

**Unchecked Return Value\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1175 |
| Status | New |

The nfsreply_print method calls the snprintf function, at line 333 of freebsd-src-2/print-nfs.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-2/print-nfs.c | freebsd-src-2/print-nfs.c |
| Line | 345 | 345 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-nfs.c
Method nfsreply_print(netdissect_options *ndo,

```
....
345.                snprintf(dstid, sizeof(dstid), "%u",
```

**Unchecked Return Value\Path 13:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1176 |
| Status | New |

The nfsreply_print method calls the snprintf function, at line 333 of freebsd-src-2/print-nfs.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-2/print-nfs.c | freebsd-src-2/print-nfs.c |
| Line | 348 | 348 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-nfs.c
Method nfsreply_print(netdissect_options *ndo,

```
....
348.              snprintf(srcid, sizeof(srcid), "%u", NFS_PORT);
```

**Unchecked Return Value\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1177 |
| Status | New |

The nfsreply_print method calls the snprintf function, at line 333 of freebsd-src-2/print-nfs.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-2/print-nfs.c | freebsd-src-2/print-nfs.c |
| Line | 349 | 349 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/print-nfs.c
Method nfsreply_print(netdissect_options *ndo,

```
....
349.              snprintf(dstid, sizeof(dstid), "%u",
```

**Unchecked Return Value\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1178 |
| Status | New |

The respip_inform_print method calls the snprintf function, at line 1291 of freebsd-src-2/respip.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-2/respip.c | freebsd-src-2/respip.c |
| Line | 1324 | 1324 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_inform_print(struct respip_action_info* respip_actinfo, uint8_t* qname,

```
....
1324.       snprintf(txt+txtlen, sizeof(txt)-txtlen,
```

**Unchecked Return Value\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1179 |
| Status | New |

The respip_rewrite_reply method calls the snprintf function, at line 866 of freebsd-src-2/respip.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-2/respip.c | freebsd-src-2/respip.c |
| Line | 966 | 966 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_rewrite_reply(const struct query_info* qinfo,

```
....
966.                                                snprintf(ip, sizeof(ip),
"invalidRRdata");
```

**Unchecked Return Value\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1180 |
| Status | New |

The make_rsid method calls the sprintf function, at line 656 of freebsd-src-2/rtsol.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-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 661 | 661 |
| Object | sprintf | sprintf |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method make_rsid(const char *ifname, const char *origin, struct rainfo *rai)

```
....
661.             sprintf(rsid, "%s:%s", ifname, origin);
```

**Unchecked Return Value\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1181 |
| Status | New |

The make_rsid method calls the sprintf function, at line 656 of freebsd-src-2/rtsol.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-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 669 | 669 |
| Object | sprintf | sprintf |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method make_rsid(const char *ifname, const char *origin, struct rainfo *rai)

```
....
669.             sprintf(rsid, "%s:%s:[%s]", ifname, origin, hbuf);
```

**Unchecked Return Value\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1182 |

| Status | New |
|---|---|

The main method calls the snprintf function, at line 470 of freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 687 | 687 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method main(int argc, char **argv)

```
....
687.        (void) snprintf(cmd, sizeof cmd, "scp%s%s%s%s",
```

**Unchecked Return Value\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1183 |
| Status | New |

The do_times method calls the snprintf function, at line 734 of freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 739 | 739 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_times(int fd, int verb, const struct stat *sb)

```
....
739.        (void)snprintf(buf, sizeof(buf), "T%llu 0 %llu 0\n",
```

**Unchecked Return Value\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1184 |
| Status | New |

The source method calls the snprintf function, at line 1378 of freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1433 | 1433 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method source(int argc, char **argv)

```
....
1433.             snprintf(buf, sizeof buf, "C%04o %lld %s\n",
```

**Unchecked Return Value\Path 22:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1185
Status New

The rsource method calls the snprintf function, at line 1490 of freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1511 | 1511 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method rsource(char *name, struct stat *statp)

```
....
1511.       (void) snprintf(path, sizeof path, "D%04o %d %.1024s\n",
```

**Unchecked Return Value\Path 23:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1186
Status New

The rsource method calls the snprintf function, at line 1490 of freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1529 | 1529 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method rsource(char *name, struct stat *statp)

```
....
1529.             (void) snprintf(path, sizeof path, "%s/%s", name, dp-
>d_name);
```

**Unchecked Return Value\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1187 |
| Status | New |

The sink method calls the snprintf function, at line 1648 of freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1819 | 1819 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1819.                   (void) snprintf(namebuf, need, "%s%s%s", targ,
```

**Unchecked Return Value\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1188 |
| Status | New |

The do_exec method calls the snprintf function, at line 657 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 680 | 680 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_exec(struct ssh *ssh, Session *s, const char *command)

```
....
680.                snprintf(session_type, sizeof(session_type),
```

**Unchecked Return Value\Path 26:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1189
Status New

The do_exec method calls the snprintf function, at line 657 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 683 | 683 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_exec(struct ssh *ssh, Session *s, const char *command)

```
....
683.                snprintf(session_type, sizeof(session_type),
```

**Unchecked Return Value\Path 27:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1190
Status New

The do_exec method calls the snprintf function, at line 657 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 686 | 686 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_exec(struct ssh *ssh, Session *s, const char *command)

```
....
686.                snprintf(session_type, sizeof(session_type), "shell");
```

**Unchecked Return Value\Path 28:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1191
Status New

The do_exec method calls the snprintf function, at line 657 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 689 | 689 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_exec(struct ssh *ssh, Session *s, const char *command)

```
....
689.                snprintf(session_type, sizeof(session_type),
"command");
```

**Unchecked Return Value\Path 29:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1192
Status New

The check_quietlogin method calls the snprintf function, at line 815 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 824 | 824 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method check_quietlogin(Session *s, const char *command)

```
....
824.        snprintf(buf, sizeof(buf), "%.200s/.hushlogin", pw->pw_dir);
```

**Unchecked Return Value\Path 30:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1193
Status New

The do_setup_env method calls the snprintf function, at line 982 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 1035 | 1035 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
1035.       snprintf(buf, sizeof buf, "%.200s/%.50s", _PATH_MAILDIR, pw-
>pw_name);
```

**Unchecked Return Value\Path 31:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1194
Status New

The do_setup_env method calls the snprintf function, at line 982 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 1138 | 1138 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
1138.             snprintf(buf, sizeof buf, "%.200s/%s/environment",
```

**Unchecked Return Value\Path 32:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1195
Status New

The do_setup_env method calls the snprintf function, at line 982 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 1182 | 1182 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
1182.       snprintf(buf, sizeof buf, "%.50s %d %d",
```

**Unchecked Return Value\Path 33:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1196
Status New

The do_setup_env method calls the snprintf function, at line 982 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 1188 | 1188 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
1188.        snprintf(buf, sizeof buf, "%.50s %d %.50s %d",
```

**Unchecked Return Value\Path 34:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1197
Status New

The do_setusercontext method calls the snprintf function, at line 1376 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 1410 | 1410 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setusercontext(struct passwd *pw)

```
....
1410.                    snprintf(uidstr, sizeof(uidstr), "%llu",
```

**Unchecked Return Value\Path 35:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1198
Status New

The session_setup_x11fwd method calls the snprintf function, at line 2589 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 2633 | 2633 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method session_setup_x11fwd(struct ssh *ssh, Session *s)

```
....
2633.             snprintf(display, sizeof display, "localhost:%u.%u",
```

**Unchecked Return Value\Path 36:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1199
Status New

The session_setup_x11fwd method calls the snprintf function, at line 2589 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 2635 | 2635 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method session_setup_x11fwd(struct ssh *ssh, Session *s)

```
....
2635.             snprintf(auth_display, sizeof auth_display,
"unix:%u.%u",
```

**Unchecked Return Value\Path 37:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1200
Status New

The session_setup_x11fwd method calls the snprintf function, at line 2589 of freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 2651 | 2651 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method session_setup_x11fwd(struct ssh *ssh, Session *s)

```
....
2651.             snprintf(display, sizeof display, "%.50s:%u.%u",
inet_ntoa(my_addr),
```

**Unchecked Return Value\Path 38:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1201
Status New

The md method calls the snprintf function, at line 59 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 62 | 62 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method md(char *buf, size_t buflen, const char *base, const char *tail)

```
....
62.   snprintf(buf, buflen, "%s/%s", base, tail);
```

**Unchecked Return Value\Path 39:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1202
Status New

The lookup_simple method calls the snprintf function, at line 67 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 73 | 73 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method lookup_simple(const atf_tc_t *tc, const char *mountpath)

```
....
73.   snprintf(pb, sizeof(pb), "%s/../%s", mountpath, basename(final));
```

**Unchecked Return Value\Path 40:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1203
Status New

The lookup_simple method calls the snprintf function, at line 67 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 77 | 77 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method lookup_simple(const atf_tc_t *tc, const char *mountpath)

```
....
77.   snprintf(pb, sizeof(pb), "%s/./../%s", mountpath,
basename(final));
```

**Unchecked Return Value\Path 41:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1204
Status New

The lookup_complex method calls the snprintf function, at line 85 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 93 | 93 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method lookup_complex(const atf_tc_t *tc, const char *mountpath)

```
....
93.   snprintf(pb, sizeof(pb), "%s/dir", mountpath);
```

**Unchecked Return Value\Path 42:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1205
Status New

The lookup_complex method calls the snprintf function, at line 85 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 99 | 99 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method lookup_complex(const atf_tc_t *tc, const char *mountpath)

```
....
99.   snprintf(pb, sizeof(pb), "%s/./dir/.././dir/.", mountpath);
```

**Unchecked Return Value\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1206
Status New

The dir_simple method calls the snprintf function, at line 156 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 164 | 164 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method dir_simple(const atf_tc_t *tc, const char *mountpath)

```
....
164.        snprintf(pb, sizeof(pb), "%s/dir", mountpath);
```

**Unchecked Return Value\Path 44:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1207
Status New

The dir_notempty method calls the snprintf function, at line 178 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 186 | 186 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method dir_notempty(const atf_tc_t *tc, const char *mountpath)

```
....
186.        snprintf(pb, sizeof(pb), "%s/dir", mountpath);
```

**Unchecked Return Value\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1208
Status New

The dir_notempty method calls the snprintf function, at line 178 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 190 | 190 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method dir_notempty(const atf_tc_t *tc, const char *mountpath)

```
....
190.        snprintf(pb2, sizeof(pb2), "%s/dir/file", mountpath);
```

**Unchecked Return Value\Path 46:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1209
Status New

The create_many method calls the snprintf function, at line 458 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 484 | 484 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method create_many(const atf_tc_t *tc, const char *mp)

```
....
484.              snprintf(buf, sizeof(buf), TESTFN "%d", i);
```

**Unchecked Return Value\Path 47:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1210
Status New

The create_many method calls the snprintf function, at line 458 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 491 | 491 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method create_many(const atf_tc_t *tc, const char *mp)

```
....
491.                snprintf(buf, sizeof(buf), TESTFN "%d", i);
```

**Unchecked Return Value\Path 48:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1211
Status New

The create_nonalphanum method calls the snprintf function, at line 507 of freebsd-src-2/t_vnops.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-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 516 | 516 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method create_nonalphanum(const atf_tc_t *tc, const char *mp)

```
....
516.                snprintf(buf, sizeof(buf), "%c", i);
```

**Unchecked Return Value\Path 49:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1212
Status New

The suboption method calls the snprintf function, at line 704 of freebsd-src-2/telnet.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-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 723 | 723 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/telnet.c
Method suboption()

```
....
723.              snprintf((char *)temp, sizeof(temp),
```

**Unchecked Return Value\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1213 |
| Status | New |

The suboption method calls the snprintf function, at line 704 of freebsd-src-2/telnet.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-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 746 | 746 |
| Object | snprintf | snprintf |

Code Snippet
File Name freebsd-src-2/telnet.c
Method suboption()

```
....
746.            snprintf((char *)temp, sizeof(temp),
```

## 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=1060098&projectid=60088&pathid=1266 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 291 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
291.          if (eigrp_tlv_len < sizeof(struct eigrp_tlv_header) ||
```

**Use of Sizeof On a Pointer Type\Path 2:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1267
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 284 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
284.          ND_TCHECK_LEN(tptr, sizeof(struct eigrp_tlv_header));
```

**Use of Sizeof On a Pointer Type\Path 3:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1268
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 293 |

| | | |
|---|---|---|
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
293.              print_unknown_data(ndo,tptr+sizeof(struct
eigrp_tlv_header),"\n\t    ",tlen);
```

**Use of Sizeof On a Pointer Type\Path 4:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1269
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 304 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
304.          if (eigrp_tlv_len < sizeof(struct eigrp_tlv_header)) {
```

**Use of Sizeof On a Pointer Type\Path 5:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1270
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 306 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c

Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
306.                              sizeof(struct eigrp_tlv_header));
```

**Use of Sizeof On a Pointer Type\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1271 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 309 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
309.          tlv_tptr=tptr+sizeof(struct eigrp_tlv_header);
```

**Use of Sizeof On a Pointer Type\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1272 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 310 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
310.          tlv_tlen=eigrp_tlv_len-sizeof(struct eigrp_tlv_header);
```

**Use of Sizeof On a Pointer Type\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1273 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 321 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
321.                      sizeof(struct eigrp_tlv_header) +
sizeof(*tlv_ptr.eigrp_tlv_general_parm));
```

**Use of Sizeof On a Pointer Type\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1274 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 338 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
338.                              sizeof(struct eigrp_tlv_header) +
sizeof(*tlv_ptr.eigrp_tlv_sw_version));
```

**Use of Sizeof On a Pointer Type\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1275 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 353 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
353.                              sizeof(struct eigrp_tlv_header) +
sizeof(*tlv_ptr.eigrp_tlv_ip_int));
```

**Use of Sizeof On a Pointer Type\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1276 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 388 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
388.                              sizeof(struct eigrp_tlv_header) +
sizeof(*tlv_ptr.eigrp_tlv_ip_ext));
```

**Use of Sizeof On a Pointer Type\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1277 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 431 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
431.                              sizeof(struct eigrp_tlv_header) +
sizeof(*tlv_ptr.eigrp_tlv_at_cable_setup));
```

**Use of Sizeof On a Pointer Type\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1278 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 445 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
445.                              sizeof(struct eigrp_tlv_header) +
sizeof(*tlv_ptr.eigrp_tlv_at_int));
```

**Use of Sizeof On a Pointer Type\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1279 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 473 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
473.                              sizeof(struct eigrp_tlv_header) +
sizeof(*tlv_ptr.eigrp_tlv_at_ext));
```

**Use of Sizeof On a Pointer Type\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1280 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 523 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
523.              print_unknown_data(ndo,tptr+sizeof(struct
eigrp_tlv_header),"\n\t    ",
```

**Use of Sizeof On a Pointer Type\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1281 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-eigrp.c | freebsd-src-2/print-eigrp.c |
| Line | 218 | 524 |
| Object | eigrp_tlv_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, const u_char *pptr, u_int len)

```
....
218.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
524.                                    eigrp_tlv_len-sizeof(struct
eigrp_tlv_header));
```

**Use of Sizeof On a Pointer Type\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1282 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-lwapp.c | freebsd-src-2/print-lwapp.c |
| Line | 170 | 230 |
| Object | lwapp_control_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-lwapp.c
Method lwapp_control_print(netdissect_options *ndo,

```
....
170.      const struct lwapp_control_header *lwapp_control_header;
....
230.          if (tlen < sizeof(struct lwapp_control_header)) {
```

**Use of Sizeof On a Pointer Type\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1283 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-lwapp.c | freebsd-src-2/print-lwapp.c |
| Line | 170 | 229 |
| Object | lwapp_control_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-lwapp.c
Method lwapp_control_print(netdissect_options *ndo,

```
....
170.      const struct lwapp_control_header *lwapp_control_header;
....
229.          ND_TCHECK_LEN(tptr, sizeof(struct lwapp_control_header));
```

**Use of Sizeof On a Pointer Type\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1284 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-lwapp.c | freebsd-src-2/print-lwapp.c |
| Line | 170 | 237 |
| Object | lwapp_control_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-lwapp.c
Method lwapp_control_print(netdissect_options *ndo,

```
....
170.      const struct lwapp_control_header *lwapp_control_header;
....
237.          if (tlen < sizeof(struct lwapp_control_header) + msg_tlen)
{
```

**Use of Sizeof On a Pointer Type\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1285 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-lwapp.c | freebsd-src-2/print-lwapp.c |
| Line | 170 | 291 |
| Object | lwapp_control_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-lwapp.c
Method lwapp_control_print(netdissect_options *ndo,

```
....
170.      const struct lwapp_control_header *lwapp_control_header;
....
291.          tptr += sizeof(struct lwapp_control_header) + msg_tlen;
```

**Use of Sizeof On a Pointer Type\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1286 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/print-lwapp.c | freebsd-src-2/print-lwapp.c |
| Line | 170 | 292 |
| Object | lwapp_control_header | sizeof |

Code Snippet
File Name freebsd-src-2/print-lwapp.c
Method lwapp_control_print(netdissect_options *ndo,

```
....
170.      const struct lwapp_control_header *lwapp_control_header;
....
292.          tlen -= sizeof(struct lwapp_control_header) + msg_tlen;
```

**Use of Sizeof On a Pointer Type\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1287 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3340 | 3350 |
| Object | marker | sizeof |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_entry_compare_acls(const char *file, int line,

```
....
3340.       int *marker;
....
3350.       marker = malloc(sizeof(marker[0]) * cnt);
```

**Use of Sizeof On a Pointer Type\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1288 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vnic_dev.c | freebsd-src-2/vnic_dev.c |
| Line | 245 | 277 |
| Object | args | sizeof |

Code Snippet
File Name freebsd-src-2/vnic_dev.c
Method static int vnic_dev_cmd_proxy(struct vnic_dev *vdev,

```
....
245.        u64 *args, int nargs, int wait)
....
277.        memcpy(args, &vdev->args[1], nargs * sizeof(args[0]));
```

**Use of Sizeof On a Pointer Type\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1289 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vnic_dev.c | freebsd-src-2/vnic_dev.c |
| Line | 245 | 262 |
| Object | args | sizeof |

Code Snippet
File Name freebsd-src-2/vnic_dev.c
Method static int vnic_dev_cmd_proxy(struct vnic_dev *vdev,

```
....
245.        u64 *args, int nargs, int wait)
....
262.        memcpy(&vdev->args[2], args, nargs * sizeof(args[0]));
```

**Use of Sizeof On a Pointer Type\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1290 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vnic_dev.c | freebsd-src-2/vnic_dev.c |
| Line | 283 | 296 |
| Object | args | sizeof |

Code Snippet
File Name freebsd-src-2/vnic_dev.c
Method static int vnic_dev_cmd_no_proxy(struct vnic_dev *vdev,

```
....
283.        enum vnic_devcmd_cmd cmd, u64 *args, int nargs, int wait)
....
296.        memcpy(args, vdev->args, nargs * sizeof(args[0]));
```

**Use of Sizeof On a Pointer Type\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1291 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vnic_dev.c | freebsd-src-2/vnic_dev.c |
| Line | 283 | 292 |
| Object | args | sizeof |

Code Snippet
File Name freebsd-src-2/vnic_dev.c
Method static int vnic_dev_cmd_no_proxy(struct vnic_dev *vdev,

```
....
283.        enum vnic_devcmd_cmd cmd, u64 *args, int nargs, int wait)
....
292.        memcpy(vdev->args, args, nargs * sizeof(args[0]));
```

**Use of Sizeof On a Pointer Type\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1292 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/acpi_thermal.c | freebsd-src-2/acpi_thermal.c |
| Line | 988 | 988 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/acpi_thermal.c
Method acpi_tz_thread(void *arg)

```
....
988.            sc = malloc(sizeof(struct acpi_tz_softc *) * devcount,
M_TEMP,
```

**Use of Sizeof On a Pointer Type\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1293 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |

| | | |
|---|---|---|
| Line | 234 | 234 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method copy_msg(struct regional* region, struct lruhash_entry* e,

```
....
234.              sizeof(struct ub_packed_rrset_key*) * rep-
>rrset_count);
```

**Use of Sizeof On a Pointer Type\Path 29:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1294
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 404 | 404 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
404.        s = sizeof(*ad) + (sizeof(size_t) + sizeof(uint8_t*) +
```

**Use of Sizeof On a Pointer Type\Path 30:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1295
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 419 | 419 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
419.        memmove(p, &d->rr_data[0], sizeof(uint8_t*)*num);
```

**Use of Sizeof On a Pointer Type\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1296 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 420 | 420 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
420.        p += sizeof(uint8_t*)*num;
```

**Use of Sizeof On a Pointer Type\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1297 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 494 | 494 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method load_rrset(RES* ssl, sldns_buffer* buf, struct worker* worker)

```
....
494.             sizeof(uint8_t*)*(d->count+d->rrsig_count));
```

**Use of Sizeof On a Pointer Type\Path 33:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1298 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cachedump.c | freebsd-src-2/cachedump.c |
| Line | 670 | 670 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/cachedump.c
Method load_msg(RES* ssl, sldns_buffer* buf, struct worker* worker)

```
....
670.                region, sizeof(struct
ub_packed_rrset_key*)*rep.rrset_count);
```

**Use of Sizeof On a Pointer Type\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1299 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/glob.c | freebsd-src-2/glob.c |
| Line | 460 | 460 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/glob.c
Method glob(const char *pattern, int flags, int (*errfunc) (const char *, int),

```
....
460.                pglob->gl_pathc - oldpathc, sizeof(char *), compare);
```

**Use of Sizeof On a Pointer Type\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1300 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |

| | | |
|---|---|---|
| Line | 620 | 620 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method showhostmap_dead(natstat_t *nsp)

```
....
620.        maptable = (hostmap_t **)malloc(sizeof(hostmap_t *) *
```

**Use of Sizeof On a Pointer Type\Path 36:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1301
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 623 | 623 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method showhostmap_dead(natstat_t *nsp)

```
....
623.                    sizeof(hostmap_t *) * nsp->ns_hostmap_sz)) {
```

**Use of Sizeof On a Pointer Type\Path 37:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1302
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 520 | 520 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_copy_rrset(const struct ub_packed_rrset_key* key, struct regional* region)

```
....
520.                (sizeof(size_t)+sizeof(uint8_t*)+sizeof(time_t));
```

**Use of Sizeof On a Pointer Type\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1303 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 998 | 998 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
998.        env = xcalloc(envsize, sizeof(char *));
```

**Use of Sizeof On a Pointer Type\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1304 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 261 | 261 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method expbrace(Char ***nvp, Char ***elp, int size)

```
....
261.                nv = xrealloc(nv, size * sizeof(Char *));
```

**Use of Sizeof On a Pointer Type\Path 40:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1305 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 303 | 303 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method globexpand(Char **v, int noglob)

```
....
303.      fnv = xmalloc(sizeof(Char ***));
```

**Use of Sizeof On a Pointer Type\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1306 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 304 | 304 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method globexpand(Char **v, int noglob)

```
....
304.      *fnv = vl = xmalloc(sizeof(Char *) * size);
```

**Use of Sizeof On a Pointer Type\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1307 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 321 | 321 |

| | | |
|---|---|---|
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method globexpand(Char **v, int noglob)

```
....
321.                    *fnv = xrealloc(*fnv, size * sizeof(Char *));
```

**Use of Sizeof On a Pointer Type\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1308
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 331 | 331 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method globexpand(Char **v, int noglob)

```
....
331.                *fnv = xrealloc(*fnv, size * sizeof(Char *));
```

**Use of Sizeof On a Pointer Type\Path 44:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1309
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 904 | 904 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method Gnmatch(const Char *string, const Char *pattern, const Char **endstr)

```
....
904.      fblk = xmalloc(sizeof(Char ***));
```

**Use of Sizeof On a Pointer Type\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1310 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 905 | 905 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method Gnmatch(const Char *string, const Char *pattern, const Char **endstr)

```
....
905.      *fblk = xmalloc(GLOBSPACE * sizeof(Char *));
```

**Use of Sizeof On a Pointer Type\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1311 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 537 | 537 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method mklist(char *buf, char *name)

```
....
537.        argv = (char **)malloc((n+3)*sizeof(char *));
```

**Use of Sizeof On a Pointer Type\Path 47:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1312 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1225 | 1225 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_contains_lines_any_order(const char *file, int line,

```
....
1225.             expected = malloc(sizeof(char *) * expected_count);
```

**Use of Sizeof On a Pointer Type\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1313 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1248 | 1248 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_contains_lines_any_order(const char *file, int line,

```
....
1248.             actual = calloc(sizeof(char *), actual_count);
```

**Use of Sizeof On a Pointer Type\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1314 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/val_utils.c | freebsd-src-2/val_utils.c |
| Line | 956 | 956 |

| | | |
|---|---|---|
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/val_utils.c
Method void val_reply_remove_auth(struct reply_info* rep, size_t index)

```
....
956.              sizeof(struct ub_packed_rrset_key*)*
```

**Use of Sizeof On a Pointer Type\Path 50:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1315
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/val_utils.c | freebsd-src-2/val_utils.c |
| Line | 993 | 993 |
| Object | sizeof | sizeof |

Code Snippet
File Name freebsd-src-2/val_utils.c
Method val_check_nonsecure(struct module_env* env, struct reply_info* rep)

```
....
993.                                  sizeof(struct ub_packed_rrset_key*)*
```

## 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=1060098&projectid=60088&pathid=1485
Status New

Method bwi_rf_map_txpower in freebsd-src-2/bwirf.c, at line 1085, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1153 | 1153 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_map_txpower(struct bwi_mac *mac)

```
....
1153.             bcopy(bwi_txpower_map_11b, rf->rf_txpower_map0,
```

**Use of Obsolete Functions\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1486 |
| Status | New |

Method bwi_rf_map_txpower in freebsd-src-2/bwirf.c, at line 1085, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1197 | 1197 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_map_txpower(struct bwi_mac *mac)

```
....
1197.                   bcopy(txpower_map, rf->rf_txpower_map0,
```

**Use of Obsolete Functions\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1487 |
| Status | New |

Method _bwi_rf_lo_update_11g in freebsd-src-2/bwirf.c, at line 1450, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1482 | 1482 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method _bwi_rf_lo_update_11g(struct bwi_mac *mac, uint16_t orig_rf7a)

```
....
1482.                                   bcopy(lo, &lo_save,
sizeof(lo_save));
```

**Use of Obsolete Functions\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1488 |
| Status | New |

Method _bwi_rf_lo_update_11g in freebsd-src-2/bwirf.c, at line 1450, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1486 | 1486 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method _bwi_rf_lo_update_11g(struct bwi_mac *mac, uint16_t orig_rf7a)

```
....
1486.                                   bcopy(lo, &lo_save,
sizeof(lo_save));
```

**Use of Obsolete Functions\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1489 |
| Status | New |

Method _bwi_rf_lo_update_11g in freebsd-src-2/bwirf.c, at line 1450, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1513 | 1513 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c

Method _bwi_rf_lo_update_11g(struct bwi_mac *mac, uint16_t orig_rf7a)

```
....
1513.                           bcopy(lo, &lo_save, sizeof(lo_save));
```

**Use of Obsolete Functions\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1490 |
| Status | New |

Method bwi_rf_lo_measure_11g in freebsd-src-2/bwirf.c, at line 1547, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1569 | 1569 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_lo_measure_11g(struct bwi_mac *mac, const struct bwi_rf_lo *src_lo,

```
....
1569.       bcopy(src_lo, &lo_min, sizeof(lo_min));
```

**Use of Obsolete Functions\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1491 |
| Status | New |

Method bwi_rf_lo_measure_11g in freebsd-src-2/bwirf.c, at line 1547, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1600 | 1600 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_lo_measure_11g(struct bwi_mac *mac, const struct bwi_rf_lo *src_lo,

```
....
1600.             bcopy(&lo_min, &lo_base, sizeof(lo_base));
```

**Use of Obsolete Functions\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1492 |
| Status | New |

Method bwi_rf_lo_measure_11g in freebsd-src-2/bwirf.c, at line 1547, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1618 | 1618 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_lo_measure_11g(struct bwi_mac *mac, const struct bwi_rf_lo *src_lo,

```
....
1618.                                   bcopy(&lo, &lo_min, sizeof(lo_min));
```

**Use of Obsolete Functions\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1493 |
| Status | New |

Method bwi_rf_lo_measure_11g in freebsd-src-2/bwirf.c, at line 1547, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1630 | 1630 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_lo_measure_11g(struct bwi_mac *mac, const struct bwi_rf_lo *src_lo,

```
....
1630.       bcopy(&lo_min, dst_lo, sizeof(*dst_lo));
```

**Use of Obsolete Functions\Path 10:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1494 |
| Status | New |

Method bwi_rf_clear_state in freebsd-src-2/bwirf.c, at line 2247, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 2265 | 2265 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/bwirf.c
Method bwi_rf_clear_state(struct bwi_rf *rf)

```
....
2265.       bcopy(rf->rf_txpower_map0, rf->rf_txpower_map,
```

**Use of Obsolete Functions\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1495 |
| Status | New |

Method ip6_output in freebsd-src-2/ip6_output.c, at line 409, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 1088 | 1088 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_output(struct mbuf *m0, struct ip6_pktopts *opt,

```
....
1088.              bcopy((fwd_tag+1), &dst_sa, sizeof(struct
sockaddr_in6));
```

**Use of Obsolete Functions\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1496 |
| Status | New |

Method ip6_copyexthdr in freebsd-src-2/ip6_output.c, at line 1297, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 1312 | 1312 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_copyexthdr(struct mbuf **mp, caddr_t hdr, int hlen)

```
....
1312.             bcopy(hdr, mtod(m, caddr_t), hlen);
```

**Use of Obsolete Functions\Path 13:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1497
Status New

Method ip6_insert_jumboopt in freebsd-src-2/ip6_output.c, at line 1322, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 1373 | 1373 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_insert_jumboopt(struct ip6_exthdrs *exthdrs, u_int32_t plen)

```
....
1373.                   bcopy(mtod(mopt, caddr_t), mtod(n, caddr_t),
```

**Use of Obsolete Functions\Path 14:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1498
Status New

Method ip6_insert_jumboopt in freebsd-src-2/ip6_output.c, at line 1322, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 1397 | 1397 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_insert_jumboopt(struct ip6_exthdrs *exthdrs, u_int32_t plen)

```
....
1397.       bcopy(&v, &optbuf[4], 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=1060098&projectid=60088&pathid=1499 |
| Status | New |

Method ip6_ctloutput in freebsd-src-2/ip6_output.c, at line 1600, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2305 | 2305 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_ctloutput(struct socket *so, struct sockopt *sopt)

```
....
2305.                           bcopy(&inp->in6p_faddr, &addr,
sizeof(addr));
```

**Use of Obsolete Functions\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1500 |
| Status | New |

Method ip6_getpcbopt in freebsd-src-2/ip6_output.c, at line 2580, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2599 | 2599 |

| | | |
|---|---|---|
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_getpcbopt(struct inpcb *inp, int optname, struct sockopt *sopt)

```
....
2599.                   bcopy(pktopt->ip6po_pktinfo, &null_pktinfo,
```

**Use of Obsolete Functions\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1501
Status New

Method ip6_getpcbopt in freebsd-src-2/ip6_output.c, at line 2580, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2615 | 2615 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_getpcbopt(struct inpcb *inp, int optname, struct sockopt *sopt)

```
....
2615.             GET_PKTOPT_EXT_HDR(ip6po_hbh);
```

**Use of Obsolete Functions\Path 18:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1502
Status New

Method ip6_getpcbopt in freebsd-src-2/ip6_output.c, at line 2580, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2618 | 2618 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c

| | |
|---|---|
| Method | ip6_getpcbopt(struct inpcb *inp, int optname, struct sockopt *sopt) |

```
....
2618.             GET_PKTOPT_EXT_HDR(ip6po_rthdr);
```

**Use of Obsolete Functions\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1503 |
| Status | New |

Method ip6_getpcbopt in freebsd-src-2/ip6_output.c, at line 2580, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2621 | 2621 |
| Object | bcopy | bcopy |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/ip6_output.c |
| Method | ip6_getpcbopt(struct inpcb *inp, int optname, struct sockopt *sopt) |

```
....
2621.             GET_PKTOPT_EXT_HDR(ip6po_dest1);
```

**Use of Obsolete Functions\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1504 |
| Status | New |

Method ip6_getpcbopt in freebsd-src-2/ip6_output.c, at line 2580, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2624 | 2624 |
| Object | bcopy | bcopy |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/ip6_output.c |
| Method | ip6_getpcbopt(struct inpcb *inp, int optname, struct sockopt *sopt) |

```
....
2624.             GET_PKTOPT_EXT_HDR(ip6po_dest2);
```

**Use of Obsolete Functions\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1505 |
| Status | New |

Method ip6_getpcbopt in freebsd-src-2/ip6_output.c, at line 2580, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2627 | 2627 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_getpcbopt(struct inpcb *inp, int optname, struct sockopt *sopt)

```
....
2627.             GET_PKTOPT_SOCKADDR(ip6po_nexthop);
```

**Use of Obsolete Functions\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1506 |
| Status | New |

Method copypktopts in freebsd-src-2/ip6_output.c, at line 2727, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2751 | 2751 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2751.             bcopy(src->ip6po_nexthop, dst->ip6po_nexthop,
```

**Use of Obsolete Functions\Path 23:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1507 |
| Status | New |

Method copypktopts in freebsd-src-2/ip6_output.c, at line 2727, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2754 | 2754 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2754.       PKTOPT_EXTHDRCPY(ip6po_hbh);
```

**Use of Obsolete Functions\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1508 |
| Status | New |

Method copypktopts in freebsd-src-2/ip6_output.c, at line 2727, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2755 | 2755 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2755.       PKTOPT_EXTHDRCPY(ip6po_dest1);
```

**Use of Obsolete Functions\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1509 |
| Status | New |

Method copypktopts in freebsd-src-2/ip6_output.c, at line 2727, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2756 | 2756 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2756.       PKTOPT_EXTHDRCPY(ip6po_dest2);
```

**Use of Obsolete Functions\Path 26:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1510
Status New

Method copypktopts in freebsd-src-2/ip6_output.c, at line 2727, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2757 | 2757 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method copypktopts(struct ip6_pktopts *dst, struct ip6_pktopts *src, int canwait)

```
....
2757.       PKTOPT_EXTHDRCPY(ip6po_rthdr); /* not copy the cached route
*/
```

**Use of Obsolete Functions\Path 27:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1511
Status New

Method ip6_setpktopt in freebsd-src-2/ip6_output.c, at line 2870, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 2986 | 2986 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
2986.            bcopy(pktinfo, opt->ip6po_pktinfo, sizeof(*pktinfo));
```

**Use of Obsolete Functions\Path 28:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1512
Status New

Method ip6_setpktopt in freebsd-src-2/ip6_output.c, at line 2870, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3072 | 3072 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3072.            bcopy(buf, opt->ip6po_nexthop, *buf);
```

**Use of Obsolete Functions\Path 29:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1513
Status New

Method ip6_setpktopt in freebsd-src-2/ip6_output.c, at line 2870, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3110 | 3110 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3110.             bcopy(hbh, opt->ip6po_hbh, hbhlen);
```

**Use of Obsolete Functions\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1514 |
| Status | New |

Method ip6_setpktopt in freebsd-src-2/ip6_output.c, at line 2870, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3177 | 3177 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3177.             bcopy(dest, *newdest, destlen);
```

**Use of Obsolete Functions\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1515 |
| Status | New |

Method ip6_setpktopt in freebsd-src-2/ip6_output.c, at line 2870, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3219 | 3219 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_setpktopt(int optname, u_char *buf, int len, struct ip6_pktopts *opt,

```
....
3219.             bcopy(rth, opt->ip6po_rthdr, rthlen);
```

**Use of Obsolete Functions\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1516 |
| Status | New |

Method ip6_splithdr in freebsd-src-2/ip6_output.c, at line 3315, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ip6_output.c | freebsd-src-2/ip6_output.c |
| Line | 3334 | 3334 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/ip6_output.c
Method ip6_splithdr(struct mbuf *m, struct ip6_exthdrs *exthdrs)

```
....
3334.             bcopy((caddr_t)ip6, mtod(m, caddr_t), sizeof(*ip6));
```

**Use of Obsolete Functions\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1517 |
| Status | New |

Method get_data in freebsd-src-2/krb5_mech.c, at line 158, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 167 | 167 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method get_data(const uint8_t **pp, size_t *lenp, struct krb5_data *dp)

```
....
167.        bcopy(*pp, dp->kd_data, sz);
```

**Use of Obsolete Functions\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1518 |
| Status | New |

Method krb5_make_token in freebsd-src-2/krb5_mech.c, at line 557, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 614 | 614 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_make_token(char tok_id[2], size_t hlen, size_t len, struct mbuf **mp)

```
....
614.        bcopy(oid->elements, p, oid->length);
```

**Use of Obsolete Functions\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1519 |
| Status | New |

Method krb5_get_mic_old in freebsd-src-2/krb5_mech.c, at line 860, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 898 | 898 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_get_mic_old(struct krb5_context *kc, struct mbuf *m,

```
....
898.        bcopy(tm->m_data, p + 8, cklen);
```

**Use of Obsolete Functions\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=600 |

| | |
|---|---|
| | 88&pathid=1520 |
| Status | New |

Method krb5_get_mic_old in freebsd-src-2/krb5_mech.c, at line 860, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 933 | 933 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_get_mic_old(struct krb5_context *kc, struct mbuf *m,

```
....
933.        bcopy(p + 8, buf, 8);
```

**Use of Obsolete Functions\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1521 |
| Status | New |

Method krb5_verify_mic_old in freebsd-src-2/krb5_mech.c, at line 1043, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1109 | 1109 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_verify_mic_old(struct krb5_context *kc, struct mbuf *m, struct mbuf *mic,

```
....
1109.       bcopy(p, tm->m_data, 8);
```

**Use of Obsolete Functions\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1522 |
| Status | New |

Method krb5_wrap_old in freebsd-src-2/krb5_mech.c, at line 1251, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1336 | 1336 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_wrap_old(struct krb5_context *kc, int conf_req_flag,

```
....
1336.       bcopy(cm->m_data, p + 8, cklen);
```

**Use of Obsolete Functions\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1523 |
| Status | New |

Method krb5_wrap_new in freebsd-src-2/krb5_mech.c, at line 1399, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1529 | 1529 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1529.            bcopy(p, tm->m_data, 16);
```

**Use of Obsolete Functions\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1524 |
| Status | New |

Method krb5_unwrap_new in freebsd-src-2/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1867 | 1867 |

| | | |
|---|---|---|
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state)

```
....
1867.                    bcopy(m->m_data, buf, RRC);
```

**Use of Obsolete Functions\Path 41:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1525
Status New

Method krb5_unwrap_new in freebsd-src-2/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1868 | 1868 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c
Method krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state)

```
....
1868.                    bcopy(m->m_data + RRC, m->m_data, rlen - RRC);
```

**Use of Obsolete Functions\Path 42:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1526
Status New

Method krb5_unwrap_new in freebsd-src-2/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1869 | 1869 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/krb5_mech.c

| | |
|---|---|
| Method | krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state) |

```
....
1869.                    bcopy(buf, m->m_data + rlen - RRC, RRC);
```

**Use of Obsolete Functions\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1527 |
| Status | New |

Method krb5_unwrap_new in freebsd-src-2/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/krb5_mech.c | freebsd-src-2/krb5_mech.c |
| Line | 1955 | 1955 |
| Object | bcopy | bcopy |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/krb5_mech.c |
| Method | krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state) |

```
....
1955.             bcopy(cm->m_data, buf, cklen);
```

**Use of Obsolete Functions\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1528 |
| Status | New |

Method vga_probe_unit in freebsd-src-2/vga.c, at line 76, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 88 | 88 |
| Object | bcopy | bcopy |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/vga.c |
| Method | vga_probe_unit(int unit, video_adapter_t *buf, int flags) |

```
....
88.   bcopy(adp, buf, sizeof(*buf));
```

**Use of Obsolete Functions\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1529 |
| Status | New |

Method update_adapter_info in freebsd-src-2/vga.c, at line 804, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 844 | 844 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/vga.c
Method update_adapter_info(video_adapter_t *adp, video_info_t *info)

```
....
844.      bcopy(info, &adp->va_info, sizeof(adp->va_info));
```

**Use of Obsolete Functions\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1530 |
| Status | New |

Method vga_set_mode in freebsd-src-2/vga.c, at line 1531, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vga.c | freebsd-src-2/vga.c |
| Line | 1549 | 1549 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/vga.c
Method vga_set_mode(video_adapter_t *adp, int mode)

```
....
1549.      bcopy(get_mode_param(mode), params.regs,
sizeof(params.regs));
```

**Use of Obsolete Functions\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1531 |
| Status | New |

Method vnic_dev_discover_res in freebsd-src-2/vnic_dev.c, at line 36, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vnic_dev.c | freebsd-src-2/vnic_dev.c |
| Line | 107 | 107 |
| Object | bcopy | bcopy |

Code Snippet
File Name freebsd-src-2/vnic_dev.c
Method static int vnic_dev_discover_res(struct vnic_dev *vdev,

```
....
107.                bcopy(&softc->mem, &vdev->res[type].bar, sizeof(softc->mem));
```

## 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=1060098&projectid=60088&pathid=1119 |
| Status | New |

The system data read by ext4_new_blocks in the file freebsd-src-2/ext2_extents.c at line 1369 is potentially exposed by ext4_new_blocks found in freebsd-src-2/ext2_extents.c at line 1369.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1370 | 1370 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_new_blocks(struct inode *ip, daddr_t lbn, e4fs_daddr_t pref,

```
....
1370.       struct ucred *cred, unsigned long *count, int *perror)
```

**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=1060098&projectid=60088&pathid=1120 |
| Status | New |

The system data read by ext4_new_blocks in the file freebsd-src-2/ext2_extents.c at line 1369 is potentially exposed by ext4_new_blocks found in freebsd-src-2/ext2_extents.c at line 1369.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1383 | 1383 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_new_blocks(struct inode *ip, daddr_t lbn, e4fs_daddr_t pref,

```
....
1383.       *perror = ext2_alloc(ip, lbn, pref, (int)fs->e2fs_bsize,
cred, &newblk);
```

**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=1060098&projectid=60088&pathid=1121 |
| Status | New |

The system data read by ext4_new_blocks in the file freebsd-src-2/ext2_extents.c at line 1369 is potentially exposed by ext4_new_blocks found in freebsd-src-2/ext2_extents.c at line 1369.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 1384 | 1384 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/ext2_extents.c
Method ext4_new_blocks(struct inode *ip, daddr_t lbn, e4fs_daddr_t pref,

```
....
1384.       if (*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=1060098&projectid=60088&pathid=1122 |
| Status | New |

The system data read by main in the file freebsd-src-2/http-server.c at line 330 is potentially exposed by main found in freebsd-src-2/http-server.c at line 330.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 389 | 389 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/http-server.c
Method main(int argc, char **argv)

```
....
389.                    perror("getsockname() failed");
```

**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=1060098&projectid=60088&pathid=1123 |
| Status | New |

The system data read by send_document_cb in the file freebsd-src-2/http-server.c at line 159 is potentially exposed by send_document_cb found in freebsd-src-2/http-server.c at line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 204 | 204 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/http-server.c
Method send_document_cb(struct evhttp_request *req, void *arg)

```
....
204.                perror("malloc");
```

**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=1060098&projectid=60088&pathid=1124 |
| Status | New |

The system data read by send_document_cb in the file freebsd-src-2/http-server.c at line 159 is potentially exposed by send_document_cb found in freebsd-src-2/http-server.c at line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 291 | 291 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/http-server.c
Method send_document_cb(struct evhttp_request *req, void *arg)

```
....
291.                    perror("open");
```

**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=1060098&projectid=60088&pathid=1125 |
| Status | New |

The system data read by send_document_cb in the file freebsd-src-2/http-server.c at line 159 is potentially exposed by send_document_cb found in freebsd-src-2/http-server.c at line 159.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 298 | 298 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/http-server.c
Method send_document_cb(struct evhttp_request *req, void *arg)

```
....
298.                    perror("fstat");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1126 |
| Status | New |

The system data read by dostats_dead in the file freebsd-src-2/ipnat.c at line 331 is potentially exposed by dostats_dead found in freebsd-src-2/ipnat.c at line 331.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 342 | 342 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method dostats_dead(natstat_t *nsp, int opts, int *filter)

```
....
342.                            perror("kmemcpy");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1127 |
| Status | New |

The system data read by showhostmap_dead in the file freebsd-src-2/ipnat.c at line 613 is potentially exposed by showhostmap_dead found in freebsd-src-2/ipnat.c at line 613.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 624 | 624 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method showhostmap_dead(natstat_t *nsp)

```
....
624.              perror("kmemcpy (maptable)");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1128 |
| Status | New |

The system data read by showhostmap_dead in the file freebsd-src-2/ipnat.c at line 613 is potentially exposed by showhostmap_dead found in freebsd-src-2/ipnat.c at line 613.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 633 | 633 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method showhostmap_dead(natstat_t *nsp)

```
....
633.                          perror("kmemcpy (hostmap)");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1129 |
| Status | New |

The system data read by do_local_cmd in the file freebsd-src-2/scp.c at line 231 is potentially exposed by do_local_cmd found in freebsd-src-2/scp.c at line 231.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 251 | 251 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_local_cmd(arglist *a)

```
....
251.                perror(a->list[0]);
```

**Exposure of System Data to Unauthorized Control Sphere\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1130 |
| Status | New |

The system data read by do_cmd in the file freebsd-src-2/scp.c at line 279 is potentially exposed by do_cmd found in freebsd-src-2/scp.c at line 279.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 352 | 352 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_cmd(char *program, char *host, char *remuser, int port, int subsystem,

```
....
352.                perror(program);
```

**Exposure of System Data to Unauthorized Control Sphere\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1131 |
| Status | New |

The system data read by do_cmd2 in the file freebsd-src-2/scp.c at line 379 is potentially exposed by do_cmd2 found in freebsd-src-2/scp.c at line 379.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 398 | 398 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_cmd2(char *host, char *remuser, int port, char *cmd,

```
....
398.                    perror("dup2");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1132 |
| Status | New |

The system data read by do_cmd2 in the file freebsd-src-2/scp.c at line 379 is potentially exposed by do_cmd2 found in freebsd-src-2/scp.c at line 379.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 400 | 400 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_cmd2(char *host, char *remuser, int port, char *cmd,

```
....
400.                    perror("dup2");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1133 |
| Status | New |

The system data read by do_cmd2 in the file freebsd-src-2/scp.c at line 379 is potentially exposed by do_cmd2 found in freebsd-src-2/scp.c at line 379.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 417 | 417 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/scp.c
Method do_cmd2(char *host, char *remuser, int port, char *cmd,

```
....
417.                perror(ssh_program);
```

**Exposure of System Data to Unauthorized Control Sphere\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1134 |
| Status | New |

The system data read by main in the file freebsd-src-2/scp.c at line 470 is potentially exposed by main found in freebsd-src-2/scp.c at line 470.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 660 | 660 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/scp.c
Method main(int argc, char **argv)

```
....
660.                    perror("pledge");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1135 |
| Status | New |

The system data read by do_exec_no_pty in the file freebsd-src-2/session.c at line 388 is potentially exposed by do_exec_no_pty found in freebsd-src-2/session.c at line 388.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 472 | 472 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_exec_no_pty(struct ssh *ssh, Session *s, const char *command)

```
....
472.                    perror("dup2 stdin");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1136 |
| Status | New |

The system data read by do_exec_no_pty in the file freebsd-src-2/session.c at line 388 is potentially exposed by do_exec_no_pty found in freebsd-src-2/session.c at line 388.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 478 | 478 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_exec_no_pty(struct ssh *ssh, Session *s, const char *command)

```
....
478.                    perror("dup2 stdout");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1137 |
| Status | New |

The system data read by do_exec_no_pty in the file freebsd-src-2/session.c at line 388 is potentially exposed by do_exec_no_pty found in freebsd-src-2/session.c at line 388.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 484 | 484 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_exec_no_pty(struct ssh *ssh, Session *s, const char *command)

```
....
484.                    perror("dup2 stderr");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1138 |
| Status | New |

The system data read by do_setusercontext in the file freebsd-src-2/session.c at line 1376 is potentially exposed by do_setusercontext found in freebsd-src-2/session.c at line 1376.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1386 | 1386 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setusercontext(struct passwd *pw)

```
....
1386.                    perror("unable to set user context");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1139 |
| Status | New |

The system data read by do_setusercontext in the file freebsd-src-2/session.c at line 1376 is potentially exposed by do_setusercontext found in freebsd-src-2/session.c at line 1376.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1425 | 1425 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_setusercontext(struct passwd *pw)

```
....
1425.                   perror("unable to set user context (setuser)");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1140 |
| Status | New |

The system data read by do_pwchange in the file freebsd-src-2/session.c at line 1459 is potentially exposed by do_pwchange found in freebsd-src-2/session.c at line 1459.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1475 | 1475 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_pwchange(Session *s)

```
....
1475.             perror("passwd");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1141 |
| Status | New |

The system data read by do_child in the file freebsd-src-2/session.c at line 1532 is potentially exposed by do_child found in freebsd-src-2/session.c at line 1532.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1710 | 1710 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1710.                   perror(shell);
```

**Exposure of System Data to Unauthorized Control Sphere\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1142 |
| Status | New |

The system data read by do_child in the file freebsd-src-2/session.c at line 1532 is potentially exposed by do_child found in freebsd-src-2/session.c at line 1532.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1720 | 1720 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1720.              perror(shell);
```

**Exposure of System Data to Unauthorized Control Sphere\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1143 |
| Status | New |

The system data read by do_child in the file freebsd-src-2/session.c at line 1532 is potentially exposed by do_child found in freebsd-src-2/session.c at line 1532.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1732 | 1732 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1732.       perror(shell);
```

**Exposure of System Data to Unauthorized Control Sphere\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1144 |
| Status | New |

The system data read by bdg_ctl in the file freebsd-src-2/valectl.c at line 204 is potentially exposed by bdg_ctl found in freebsd-src-2/valectl.c at line 204.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 220 | 220 |
| Object | perror | perror |

Code Snippet
File Name freebsd-src-2/valectl.c
Method bdg_ctl(struct args *a)

```
....
220.              perror("/dev/netmap");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1145 |
| Status | New |

The system data read by main in the file freebsd-src-2/ipnat.c at line 92 is potentially exposed by main found in freebsd-src-2/ipnat.c at line 92.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 185 | 184 |
| Object | errno | fprintf |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method main(int argc, char *argv[])

```
....
185.                            STRERROR(errno));
....
184.                      (void) fprintf(stderr, "%s: open: %s\n",
IPNAT_NAME,
```

**Exposure of System Data to Unauthorized Control Sphere\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1146 |
| Status | New |

The system data read by do_child in the file freebsd-src-2/session.c at line 1532 is potentially exposed by do_child found in freebsd-src-2/session.c at line 1532.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1650 | 1648 |
| Object | errno | fprintf |

Code Snippet
File Name freebsd-src-2/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1650.                          strerror(errno));
....
1648.                     fprintf(stderr, "Could not chdir to home "
```

**Exposure of System Data to Unauthorized Control Sphere\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1147 |
| Status | New |

The system data read by list_all in the file freebsd-src-2/valectl.c at line 180 is potentially exposed by list_all found in freebsd-src-2/valectl.c at line 180.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 193 | 193 |
| Object | errno | fprintf |

Code Snippet
File Name freebsd-src-2/valectl.c

| | |
|---|---|
| Method | list_all(int fd, struct nmreq_header *hdr) |

```
....
193.                    fprintf(stderr, "failed to list all: %s\n",
strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1148 |
| Status | New |

The system data read by bdg_ctl in the file freebsd-src-2/valectl.c at line 204 is potentially exposed by bdg_ctl found in freebsd-src-2/valectl.c at line 204.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 304 | 303 |
| Object | errno | fprintf |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/valectl.c |
| Method | bdg_ctl(struct args *a) |

```
....
304.                            action, a->name, strerror(errno));
....
303.              fprintf(stderr, "failed to %s %s: %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1149 |
| Status | New |

The system data read by wlan_ioctl_init in the file freebsd-src-2/wlan_sys.c at line 96 is potentially exposed by wlan_ioctl_init found in freebsd-src-2/wlan_sys.c at line 96.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 99 | 99 |
| Object | errno | strerror |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/wlan_sys.c |

| | |
|---|---|
| Method | wlan_ioctl_init(void) |

```
....
99.         syslog(LOG_ERR, "cannot open socket : %s", strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1150 |
| Status | New |

The system data read by wlan_get_local_addr in the file freebsd-src-2/wlan_sys.c at line 286 is potentially exposed by wlan_get_local_addr found in freebsd-src-2/wlan_sys.c at line 286.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 295 | 295 |
| Object | errno | strerror |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/wlan_sys.c |
| Method | wlan_get_local_addr(struct wlan_iface *wif) |

```
....
295.                    strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1151 |
| Status | New |

The system data read by wlan_clone_create in the file freebsd-src-2/wlan_sys.c at line 718 is potentially exposed by wlan_clone_create found in freebsd-src-2/wlan_sys.c at line 718.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 783 | 783 |
| Object | errno | strerror |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/wlan_sys.c |
| Method | wlan_clone_create(struct wlan_iface *wif) |

```
....
783.                    "failed: %s", strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1152 |
| Status | New |

The system data read by wlan_clone_destroy in the file freebsd-src-2/wlan_sys.c at line 791 is potentially exposed by wlan_clone_destroy found in freebsd-src-2/wlan_sys.c at line 791.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/wlan_sys.c | freebsd-src-2/wlan_sys.c |
| Line | 803 | 803 |
| Object | errno | strerror |

Code Snippet
File Name freebsd-src-2/wlan_sys.c
Method wlan_clone_destroy(struct wlan_iface *wif)

```
....
803.                    "failed: %s", strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1153 |
| Status | New |

The system data read by main in the file freebsd-src-2/zinject.c at line 737 is potentially exposed by main found in freebsd-src-2/zinject.c at line 737.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/zinject.c | freebsd-src-2/zinject.c |
| Line | 765 | 765 |
| Object | errno | fprintf |

Code Snippet
File Name freebsd-src-2/zinject.c
Method main(int argc, char **argv)

```
....
765.              (void) fprintf(stderr, "%s\n",
libzfs_error_init(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1154 |
| Status | New |

The system data read by iter_handlers in the file freebsd-src-2/zinject.c at line 336 is potentially exposed by iter_handlers found in freebsd-src-2/zinject.c at line 336.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/zinject.c | freebsd-src-2/zinject.c |
| Line | 349 | 348 |
| Object | errno | fprintf |

Code Snippet
File Name freebsd-src-2/zinject.c
Method iter_handlers(int (*func)(int, const char *, zinject_record_t *, void *),

```
....
349.                  strerror(errno));
....
348.              (void) fprintf(stderr, "Unable to list handlers:
%s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1155 |
| Status | New |

The system data read by cancel_one_handler in the file freebsd-src-2/zinject.c at line 502 is potentially exposed by cancel_one_handler found in freebsd-src-2/zinject.c at line 502.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/zinject.c | freebsd-src-2/zinject.c |
| Line | 512 | 511 |
| Object | errno | fprintf |

Code Snippet
File Name freebsd-src-2/zinject.c
Method cancel_one_handler(int id, const char *pool, zinject_record_t *record,

```
....
512.                    id, strerror(errno));
....
511.                (void) fprintf(stderr, "failed to remove handler %d:
%s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1156 |
| Status | New |

The system data read by cancel_handler in the file freebsd-src-2/zinject.c at line 537 is potentially exposed by cancel_handler found in freebsd-src-2/zinject.c at line 537.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/zinject.c | freebsd-src-2/zinject.c |
| Line | 545 | 544 |
| Object | errno | fprintf |

Code Snippet
File Name freebsd-src-2/zinject.c
Method cancel_handler(int id)

```
....
545.                    id, strerror(errno));
....
544.                (void) fprintf(stderr, "failed to remove handler %d:
%s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1157 |
| Status | New |

The system data read by register_handler in the file freebsd-src-2/zinject.c at line 558 is potentially exposed by register_handler found in freebsd-src-2/zinject.c at line 558.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/zinject.c | freebsd-src-2/zinject.c |
| Line | 570 | 568 |
| Object | errno | fprintf |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/zinject.c |
| Method | register_handler(const char *pool, int flags, zinject_record_t *record, |

```
....
570.                    strerror(errno));
....
568.                (void) fprintf(stderr, "failed to add handler: %s\n",
```

## 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=1060098&projectid=60088&pathid=1082 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1836 | 1836 |
| Object | chmod | chmod |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/scp.c |
| Method | sink(int argc, char **argv, const char *src) |

```
....
1836.                                   (void) chmod(np, mode);
```

**Incorrect Permission Assignment For Critical Resources\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1083 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1850 | 1850 |

| | | |
|---|---|---|
| Object | chmod | chmod |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1850.                           (void) chmod(vect[0], mode);
```

**Incorrect Permission Assignment For Critical Resources\Path 3:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1084
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 605 | 605 |
| Object | chmod | chmod |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_chmod(const char *file, int line, const char *pathname, int mode)

```
....
605.        if (chmod(pathname, mode) == 0)
```

**Incorrect Permission Assignment For Critical Resources\Path 4:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1085
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 149 | 149 |
| Object | _umask | _umask |

Code Snippet
File Name freebsd-src-2/test_main.c
Method mode_t umasked(mode_t expected_mode)

```
....
149.        mode_t mode = umask(0);
```

**Incorrect Permission Assignment For Critical Resources\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1086 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 150 | 150 |
| Object | _umask | _umask |

Code Snippet
File Name freebsd-src-2/test_main.c
Method mode_t umasked(mode_t expected_mode)

```
....
150.        umask(mode);
```

**Incorrect Permission Assignment For Critical Resources\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1087 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 2065 | 2065 |
| Object | _umask | _umask |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_umask(const char *file, int line, int mask)

```
....
2065.       umask(mask);
```

**Incorrect Permission Assignment For Critical Resources\Path 7:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1088 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3566 | 3566 |
| Object | _umask | _umask |

Code Snippet
File Name freebsd-src-2/test_main.c
Method test_run(int i, const char *tmpdir)

```
....
3566.        umask(oldumask = umask(0));
```

**Incorrect Permission Assignment For Critical Resources\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1089 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3566 | 3566 |
| Object | _umask | _umask |

Code Snippet
File Name freebsd-src-2/test_main.c
Method test_run(int i, const char *tmpdir)

```
....
3566.        umask(oldumask = umask(0));
```

**Incorrect Permission Assignment For Critical Resources\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1090 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3576 | 3576 |

| | | |
|---|---|---|
| Object | _umask | _umask |

Code Snippet
File Name freebsd-src-2/test_main.c
Method test_run(int i, const char *tmpdir)

```
....
3576.        umask(oldumask);
```

**Incorrect Permission Assignment For Critical Resources\Path 10:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1091
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cut.c | freebsd-src-2/cut.c |
| Line | 149 | 149 |
| Object | fp | fp |

Code Snippet
File Name freebsd-src-2/cut.c
Method main(int argc, char *argv[])

```
....
149.                            if (!(fp = fopen(*argv, "r"))) {
```

**Incorrect Permission Assignment For Critical Resources\Path 11:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1092
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/diff.c | freebsd-src-2/diff.c |
| Line | 497 | 497 |
| Object | fp | fp |

Code Snippet
File Name freebsd-src-2/diff.c
Method read_excludes_file(char *file)

```
....
497.        else if ((fp = fopen(file, "r")) == NULL)
```

**Incorrect Permission Assignment For Critical Resources\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1093 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/gethostid.c | freebsd-src-2/gethostid.c |
| Line | 46 | 46 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/gethostid.c
Method get_spl_hostid(void)

```
....
46.    f = fopen("/proc/sys/kernel/spl/hostid", "re");
```

**Incorrect Permission Assignment For Critical Resources\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1094 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 132 | 132 |
| Object | fp | fp |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
132.        if ((fp = fopen(argv[1], "r")) == NULL) {
```

**Incorrect Permission Assignment For Critical Resources\Path 14:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1095 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 797 | 797 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/session.c
Method do_motd(void)

```
....
797.                f = fopen(login_getcapstr(lc, "welcome", "/etc/motd",
```

**Incorrect Permission Assignment For Critical Resources\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1096 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 852 | 852 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/session.c
Method read_environment_file(char ***env, u_int *envsize,

```
....
852.        f = fopen(filename, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1097 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 1312 | 1312 |

| | | |
|---|---|---|
| Object | f | f |

Code Snippet
File Name freebsd-src-2/session.c
Method do_nologin(struct passwd *pw)

```
....
1312.       if ((f = fopen(nl, "r")) != NULL) {
```

**Incorrect Permission Assignment For Critical Resources\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1098
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 986 | 986 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_empty_file(const char *filename, int line, const char *f1)

```
....
986.        f = fopen(f1, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 18:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1099
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1033 | 1033 |
| Object | f1 | f1 |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_equal_file(const char *filename, int line, const char *fn1, const char *fn2)

```
....
1033.       f1 = fopen(fn1, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1100 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1034 | 1034 |
| Object | f2 | f2 |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_equal_file(const char *filename, int line, const char *fn1, const char *fn2)

```
....
1034.       f2 = fopen(fn2, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1101 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1108 | 1108 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_contents(const char *filename, int line, const void *buff, int s, const char *fn)

```
....
1108.       f = fopen(fn, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 21:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1102 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1145 | 1145 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_text_file_contents(const char *filename, int line, const char *buff, const char *fn)

```
....
1145.        f = fopen(fn, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1103 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1941 | 1941 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_make_file(const char *file, int line,

```
....
1941.        f = fopen(path, "wb");
```

**Incorrect Permission Assignment For Critical Resources\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1104 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3101 | 3101 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/test_main.c
Method slurpfile(size_t * sizep, const char *fmt, ...)

```
....
3101.       f = fopen(filename, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 24:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1105
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3144 | 3144 |
| Object | f | f |

Code Snippet
File Name freebsd-src-2/test_main.c
Method dumpfile(const char *filename, void *data, size_t len)

```
....
3144.       f = fopen(filename, "wb");
```

**Incorrect Permission Assignment For Critical Resources\Path 25:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1106
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3166 | 3166 |
| Object | in | in |

Code Snippet
File Name freebsd-src-2/test_main.c
Method extract_reference_file(const char *name)

```
....
3166.       in = fopen(buff, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1107 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3181 | 3181 |
| Object | out | out |

Code Snippet
File Name freebsd-src-2/test_main.c
Method extract_reference_file(const char *name)

```
....
3181.       out = fopen(name, "wb");
```

**Incorrect Permission Assignment For Critical Resources\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1108 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3225 | 3225 |
| Object | in | in |

Code Snippet
File Name freebsd-src-2/test_main.c
Method copy_reference_file(const char *name)

```
....
3225.       in = fopen(buff, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 28:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1109 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3232 | 3232 |
| Object | out | out |

Code Snippet
File Name freebsd-src-2/test_main.c
Method copy_reference_file(const char *name)

```
....
3232.        out = fopen(name, "wb");
```

**Incorrect Permission Assignment For Critical Resources\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1110 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3552 | 3552 |
| Object | logfile | logfile |

Code Snippet
File Name freebsd-src-2/test_main.c
Method test_run(int i, const char *tmpdir)

```
....
3552.        logfile = fopen(logfilename, "w");
```

**Incorrect Permission Assignment For Critical Resources\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1111 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1596 | 1596 |

| | | |
|---|---|---|
| Object | mkdir | mkdir |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink_sftp(int argc, char *dst, const char *src, struct sftp_conn *conn)

```
....
1596.             if (mkdir(dst, 0777) != 0) {
```

**Incorrect Permission Assignment For Critical Resources\Path 31:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1112
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 1840 | 1840 |
| Object | mkdir | mkdir |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1840.                         if (mkdir(np, mode | S_IRWXU) == -1)
```

**Incorrect Permission Assignment For Critical Resources\Path 32:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1113
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/templates_test.cpp | freebsd-src-2/templates_test.cpp |
| Line | 941 | 941 |
| Object | mkdir | mkdir |

Code Snippet
File Name freebsd-src-2/templates_test.cpp
Method ATF_TEST_CASE_BODY(instantiate__files__output_error)

```
....
941.      fs::mkdir(fs::path("dir"), 0444);
```

**Incorrect Permission Assignment For Critical Resources\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1114 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1916 | 1916 |
| Object | _mkdir | _mkdir |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_make_dir(const char *file, int line, const char *dirname, int mode)

```
....
1916.       if (0 == _mkdir(dirname))
```

**Incorrect Permission Assignment For Critical Resources\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1115 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 330 | 330 |
| Object | CreateFile | CreateFile |

Code Snippet
File Name freebsd-src-2/test_main.c
Method my_GetFileInformationByName(const char *path, BY_HANDLE_FILE_INFORMATION *bhfi)

```
....
330.        h = CreateFile(path, FILE_READ_ATTRIBUTES, 0, NULL,
```

**Incorrect Permission Assignment For Critical Resources\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1116 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1435 | 1435 |
| Object | CreateFile | CreateFile |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_file_time(const char *file, int line,

```
....
1435.       h = CreateFile(pathname, FILE_READ_ATTRIBUTES, 0, NULL,
```

**Incorrect Permission Assignment For Critical Resources\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1117 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1767 | 1767 |
| Object | CreateFileA | CreateFileA |

Code Snippet
File Name freebsd-src-2/test_main.c
Method is_symlink(const char *file, int line,

```
....
1767.       h = CreateFileA(pn, 0, FILE_SHARE_READ, NULL, OPEN_EXISTING,
```

**Incorrect Permission Assignment For Critical Resources\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1118 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |

| | | |
|---|---|---|
| Line | 2085 | 2085 |
| Object | CreateFileA | CreateFileA |

Code Snippet
File Name freebsd-src-2/test_main.c
Method assertion_utimes(const char *file, int line,

```
....
2085.       h = CreateFileA(pathname,GENERIC_READ | GENERIC_WRITE,
```

## 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=1060098&projectid=60088&pathid=1573 |
| Status | New |

The main method in freebsd-src-2/cut.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-2/cut.c | freebsd-src-2/cut.c |
| Line | 149 | 149 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/cut.c
Method main(int argc, char *argv[])

```
....
149.                            if (!(fp = fopen(*argv, "r"))) {
```

**TOCTOU\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1574 |
| Status | New |

The read_excludes_file method in freebsd-src-2/diff.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-2/diff.c | freebsd-src-2/diff.c |
| Line | 497 | 497 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/diff.c
Method read_excludes_file(char *file)

```
....
497.        else if ((fp = fopen(file, "r")) == NULL)
```

**TOCTOU\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1575 |
| Status | New |

The get_spl_hostid method in freebsd-src-2/gethostid.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-2/gethostid.c | freebsd-src-2/gethostid.c |
| Line | 46 | 46 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/gethostid.c
Method get_spl_hostid(void)

```
....
46.    f = fopen("/proc/sys/kernel/spl/hostid", "re");
```

**TOCTOU\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1576 |
| Status | New |

The main method in freebsd-src-2/maketab.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-2/maketab.c | freebsd-src-2/maketab.c |
| Line | 132 | 132 |

| | | |
|---|---|---|
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/maketab.c
Method int main(int argc, char *argv[])

```
....
132.        if ((fp = fopen(argv[1], "r")) == NULL) {
```

**TOCTOU\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1577 |
| Status | New |

The do_motd method in freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 797 | 797 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/session.c
Method do_motd(void)

```
....
797.              f = fopen(login_getcapstr(lc, "welcome", "/etc/motd",
```

**TOCTOU\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1578 |
| Status | New |

The read_environment_file method in freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 852 | 852 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/session.c
Method read_environment_file(char ***env, u_int *envsize,

```
....
852.        f = fopen(filename, "r");
```

**TOCTOU\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1579 |
| Status | New |

The do_nologin method in freebsd-src-2/session.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-2/session.c | freebsd-src-2/session.c |
| Line | 1312 | 1312 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/session.c
Method do_nologin(struct passwd *pw)

```
....
1312.       if ((f = fopen(nl, "r")) != NULL) {
```

**TOCTOU\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1580 |
| Status | New |

The assertion_empty_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 986 | 986 |
| Object | fopen | fopen |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/test_main.c |
| Method | assertion_empty_file(const char *filename, int line, const char *f1) |

```
....
986.        f = fopen(f1, "rb");
```

**TOCTOU\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1581 |
| Status | New |

The assertion_equal_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1033 | 1033 |
| Object | fopen | fopen |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/test_main.c |
| Method | assertion_equal_file(const char *filename, int line, const char *fn1, const char *fn2) |

```
....
1033.       f1 = fopen(fn1, "rb");
```

**TOCTOU\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1582 |
| Status | New |

The assertion_equal_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1034 | 1034 |
| Object | fopen | fopen |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/test_main.c |
| Method | assertion_equal_file(const char *filename, int line, const char *fn1, const char *fn2) |

```
....
1034.       f2 = fopen(fn2, "rb");
```

**TOCTOU\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1583 |
| Status | New |

The assertion_file_contents method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1108 | 1108 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/test_main.c |
| Method | assertion_file_contents(const char *filename, int line, const void *buff, int s, const char *fn) |

```
....
1108.       f = fopen(fn, "rb");
```

**TOCTOU\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1584 |
| Status | New |

The assertion_text_file_contents method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1145 | 1145 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/test_main.c |
| Method | assertion_text_file_contents(const char *filename, int line, const char *buff, const char *fn) |

```
....
1145.       f = fopen(fn, "r");
```

**TOCTOU\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1585 |
| Status | New |

The assertion_make_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 1941 | 1941 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/test_main.c |
| Method | assertion_make_file(const char *file, int line, |

```
....
1941.       f = fopen(path, "wb");
```

**TOCTOU\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1586 |
| Status | New |

The slurpfile method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3101 | 3101 |
| Object | fopen | fopen |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/test_main.c |
| Method | slurpfile(size_t * sizep, const char *fmt, ...) |

```
....
3101.       f = fopen(filename, "rb");
```

**TOCTOU\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1587 |
| Status | New |

The dumpfile method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3144 | 3144 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/test_main.c |
| Method | dumpfile(const char *filename, void *data, size_t len) |

```
....
3144.       f = fopen(filename, "wb");
```

**TOCTOU\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1588 |
| Status | New |

The extract_reference_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3166 | 3166 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/test_main.c |
| Method | extract_reference_file(const char *name) |

```
....
3166.       in = fopen(buff, "r");
```

**TOCTOU\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1589 |
| Status | New |

The extract_reference_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3181 | 3181 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/test_main.c
Method extract_reference_file(const char *name)

```
....
3181.       out = fopen(name, "wb");
```

**TOCTOU\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1590 |
| Status | New |

The copy_reference_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3225 | 3225 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/test_main.c
Method copy_reference_file(const char *name)

```
....
3225.       in = fopen(buff, "rb");
```

**TOCTOU\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1591 |
| Status | New |

The copy_reference_file method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3232 | 3232 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/test_main.c
Method copy_reference_file(const char *name)

```
....
3232.       out = fopen(name, "wb");
```

**TOCTOU\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1592 |
| Status | New |

The test_run method in freebsd-src-2/test_main.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-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3552 | 3552 |
| Object | fopen | fopen |

Code Snippet
File Name freebsd-src-2/test_main.c
Method test_run(int i, const char *tmpdir)

```
....
3552.       logfile = fopen(logfilename, "w");
```

**TOCTOU\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1593 |
| Status | New |

The get_system_hostid method in freebsd-src-2/gethostid.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-2/gethostid.c | freebsd-src-2/gethostid.c |
| Line | 71 | 71 |
| Object | open | open |

Code Snippet
File Name freebsd-src-2/gethostid.c
Method get_system_hostid(void)

```
....
71.         int fd = open("/etc/hostid", O_RDONLY | O_CLOEXEC);
```

**TOCTOU\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1594 |
| Status | New |

The main method in freebsd-src-2/ipnat.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-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 182 | 182 |
| Object | open | open |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method main(int argc, char *argv[])

```
....
182.              if (((fd = open(IPNAT_NAME, mode)) == -1) &&
```

**TOCTOU\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1595 |
| Status | New |

The main method in freebsd-src-2/ipnat.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-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 183 | 183 |
| Object | open | open |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method main(int argc, char *argv[])

```
....
183.                  ((fd = open(IPNAT_NAME, O_RDONLY)) == -1)) {
```

**TOCTOU\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1596 |
| Status | New |

The source method in freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1395 | 1395 |
| Object | open | open |

Code Snippet
File Name freebsd-src-2/scp.c
Method source(int argc, char **argv)

```
....
1395.             if ((fd = open(name, O_RDONLY|O_NONBLOCK)) == -1)
```

**TOCTOU\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1597 |
| Status | New |

The sink method in freebsd-src-2/scp.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-2/scp.c | freebsd-src-2/scp.c |
| Line | 1856 | 1856 |
| Object | open | open |

Code Snippet
File Name freebsd-src-2/scp.c
Method sink(int argc, char **argv, const char *src)

```
....
1856.             if ((ofd = open(np, O_WRONLY|O_CREAT, mode)) == -1) {
```

**TOCTOU\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1598 |
| Status | New |

The bdg_ctl method in freebsd-src-2/valectl.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-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 218 | 218 |
| Object | open | open |

Code Snippet
File Name freebsd-src-2/valectl.c
Method bdg_ctl(struct args *a)

```
....
218.        fd = open("/dev/netmap", O_RDWR);
```

**TOCTOU\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1599 |
| Status | New |

The main method in freebsd-src-2/zinject.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-2/zinject.c | freebsd-src-2/zinject.c |
| Line | 771 | 771 |
| Object | open | open |

Code Snippet
File Name freebsd-src-2/zinject.c
Method main(int argc, char **argv)

```
....
771.        if ((zfs_fd = open(ZFS_DEV, O_RDWR)) < 0) {
```

## 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=1060098&projectid=60088&pathid=1533 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3862 | 3862 |
| Object | tests | sizeof |

Code Snippet
File Name freebsd-src-2/test_main.c
Method main(int argc, char **argv)

```
....
3862.       static const int limit = sizeof(tests) / sizeof(tests[0]);
```

**Sizeof Pointer Argument\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1534 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/vt_vga.c | freebsd-src-2/vt_vga.c |
| Line | 542 | 542 |
| Object | planes | sizeof |

Code Snippet
File Name freebsd-src-2/vt_vga.c
Method vga_bitblt_pixels_block_ncolors(struct vt_device *vd, const uint8_t *masks,

```
....
542.        memset(planes, 0, sizeof(planes));
```

**Sizeof Pointer Argument\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1535 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 978 | 978 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
978.        if (NETROOM() > sizeof(str_lm)) {
```

**Sizeof Pointer Argument\Path 4:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1536 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 978 | 978 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
978.        if (NETROOM() > sizeof(str_lm)) {
```

**Sizeof Pointer Argument\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1537 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1014 | 1014 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
1014.       if (NETROOM() > sizeof(str_lm)) {
```

**Sizeof Pointer Argument\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1538 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1014 | 1014 |

| | | |
|---|---|---|
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
1014.       if (NETROOM() > sizeof(str_lm)) {
```

**Sizeof Pointer Argument\Path 7:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1539
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/util-print.c | freebsd-src-2/util-print.c |
| Line | 663 | 663 |
| Object | bitmasks | sizeof |

Code Snippet
File Name freebsd-src-2/util-print.c
Method mask62plen(const u_char *mask)

```
....
663.              for (bits = 0; bits < (sizeof (bitmasks) / sizeof
(bitmasks[0])); bits++) {
```

**Sizeof Pointer Argument\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1540
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/util-print.c | freebsd-src-2/util-print.c |
| Line | 663 | 663 |
| Object | bitmasks | sizeof |

Code Snippet
File Name freebsd-src-2/util-print.c
Method mask62plen(const u_char *mask)

```
....
663.              for (bits = 0; bits < (sizeof (bitmasks) / sizeof
(bitmasks[0])); bits++) {
```

**Sizeof Pointer Argument\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1541 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 979 | 979 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
979.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1542 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 978 | 979 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
978.        if (NETROOM() > sizeof(str_lm)) {
979.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 11:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1543 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 979 | 979 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
979.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1544 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 978 | 979 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
978.        if (NETROOM() > sizeof(str_lm)) {
979.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1545 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1015 | 1015 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
1015.           ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 14:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1546
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1014 | 1015 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
1014.       if (NETROOM() > sizeof(str_lm)) {
1015.           ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 15:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1547
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1015 | 1015 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c

Method lm_do(unsigned char *cmd, int len)

```
....
1015.           ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 16:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1548
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1014 | 1015 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
1014.       if (NETROOM() > sizeof(str_lm)) {
1015.           ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

**Sizeof Pointer Argument\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1549
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 980 | 980 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
980.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

**Sizeof Pointer Argument\Path 18:**

Severity Low

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1550 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 978 | 980 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
978.        if (NETROOM() > sizeof(str_lm)) {
....
980.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

**Sizeof Pointer Argument\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1551 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 980 | 980 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
980.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

**Sizeof Pointer Argument\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1552 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 978 | 980 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
978.        if (NETROOM() > sizeof(str_lm)) {
....
980.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

**Sizeof Pointer Argument\Path 21:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1553
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1016 | 1016 |
| Object | str_lm | sizeof |

Code Snippet
File Name freebsd-src-2/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
1016.           printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

**Sizeof Pointer Argument\Path 22:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1554
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1014 | 1016 |
| Object | str_lm | sizeof |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/telnet.c |
| Method | lm_do(unsigned char *cmd, int len) |

```
....
1014.       if (NETROOM() > sizeof(str_lm)) {
....
1016.           printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

**Sizeof Pointer Argument\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1555 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1016 | 1016 |
| Object | str_lm | sizeof |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/telnet.c |
| Method | lm_do(unsigned char *cmd, int len) |

```
....
1016.           printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

**Sizeof Pointer Argument\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1556 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/telnet.c | freebsd-src-2/telnet.c |
| Line | 1014 | 1016 |
| Object | str_lm | sizeof |

Code Snippet

| | |
|---|---|
| File Name | freebsd-src-2/telnet.c |
| Method | lm_do(unsigned char *cmd, int len) |

```
....
1014.       if (NETROOM() > sizeof(str_lm)) {
....
1016.           printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

## 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=1060098&projectid=60088&pathid=1557 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bn_gf2m.c | freebsd-src-2/bn_gf2m.c |
| Line | 373 | 373 |
| Object | n | n |

Code Snippet
File Name freebsd-src-2/bn_gf2m.c
Method int BN_GF2m_mod_arr(BIGNUM *r, const BIGNUM *a, const int p[])

```
....
373.              z[n] ^= (zz << d0);
```

**Unchecked Array Index\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1558 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/bwirf.c | freebsd-src-2/bwirf.c |
| Line | 1025 | 1025 |
| Object | idx | idx |

Code Snippet
File Name freebsd-src-2/bwirf.c

| | |
|---|---|
| Method | bwi_rf_calibval(struct bwi_mac *mac) |

```
....
1025.       calib = rf_calibvals[idx] << 1;
```

**Unchecked Array Index\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1559 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/http-server.c | freebsd-src-2/http-server.c |
| Line | 237 | 237 |
| Object | dirlen | dirlen |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/http-server.c |
| Method | send_document_cb(struct evhttp_request *req, void *arg) |

```
....
237.              pattern[dirlen] = '\\';
```

**Unchecked Array Index\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1560 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/qmi.c | freebsd-src-2/qmi.c |
| Line | 341 | 341 |
| Object | j | j |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/qmi.c |
| Method | static int ath10k_qmi_send_cal_report_req(struct ath10k_qmi *qmi) |

```
....
341.                    req.meta_data[j] = qmi->cal_data[i].cal_id;
```

**Unchecked Array Index\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1561 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 729 | 729 |
| Object | rrset_id | rrset_id |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_data_answer(enum respip_action action,

```
....
729.        new_rep->rrsets[rrset_id] = rp;
```

**Unchecked Array Index\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1562 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 1076 | 1076 |
| Object | id | id |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1076.                   qstate->minfo[id] = rq;
```

**Unchecked Array Index\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1563 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |

| | | |
|---|---|---|
| Line | 1079 | 1079 |
| Object | id | id |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1079.                   qstate->ext_state[id] = module_finished;
```

**Unchecked Array Index\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1564
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 1083 | 1083 |
| Object | id | id |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1083.               qstate->ext_state[id] = module_wait_module;
```

**Unchecked Array Index\Path 9:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1565
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 1136 | 1136 |
| Object | id | id |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1136.             qstate->ext_state[id] = next_state;
```

**Unchecked Array Index\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1566 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 1138 | 1138 |
| Object | id | id |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1138.             qstate->ext_state[id] = module_finished;
```

**Unchecked Array Index\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1567 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/respip.c | freebsd-src-2/respip.c |
| Line | 1246 | 1246 |
| Object | id | id |

Code Snippet
File Name freebsd-src-2/respip.c
Method respip_clear(struct module_qstate* qstate, int id)

```
....
1246.       qstate->minfo[id] = NULL;
```

**Unchecked Array Index\Path 12:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1568 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 843 | 843 |
| Object | wcid | wcid |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_newassoc(struct ieee80211_node *ni, int isnew)

```
....
843.                sc->wcid2ni[wcid] = ni;
```

**Unchecked Array Index\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1569 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 1673 | 1673 |
| Object | cur | cur |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_tx(struct rt2860_softc *sc, struct mbuf *m, struct ieee80211_node *ni)

```
....
1673.        ring->data[ring->cur] = data;
```

**Unchecked Array Index\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1570 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rt2860.c | freebsd-src-2/rt2860.c |
| Line | 1916 | 1916 |

| | | |
|---|---|---|
| Object | cur | cur |

Code Snippet
File Name freebsd-src-2/rt2860.c
Method rt2860_tx_raw(struct rt2860_softc *sc, struct mbuf *m,

```
....
1916.        ring->data[ring->cur] = data;
```

**Unchecked Array Index\Path 15:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1571
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 863 | 863 |
| Object | o | o |

Code Snippet
File Name freebsd-src-2/scp.c
Method emit_expansion(const char *pattern, int brace_start, int brace_end,

```
....
863.        cp[o] = '\0';
```

**Unchecked Array Index\Path 16:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1572
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/t_vnops.c | freebsd-src-2/t_vnops.c |
| Line | 654 | 654 |
| Object | len | len |

Code Snippet
File Name freebsd-src-2/t_vnops.c
Method symlink_len(const atf_tc_t *tc, const char *mp, size_t len)

```
....
654.        buf[len] = '\0';
```

## 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=1060098&projectid=60088&pathid=200 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/cut.c | freebsd-src-2/cut.c |
| Line | 91 | 91 |
| Object | getopt | getopt |

Code Snippet
File Name freebsd-src-2/cut.c
Method main(int argc, char *argv[])

```
....
91.   while ((ch = getopt(argc, argv, "b:c:d:f:snw")) != -1)
```

**Inconsistent Implementations\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=201 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/ipnat.c | freebsd-src-2/ipnat.c |
| Line | 110 | 110 |
| Object | getopt | getopt |

Code Snippet
File Name freebsd-src-2/ipnat.c
Method main(int argc, char *argv[])

```
....
110.        while ((c = getopt(argc, argv, "CdFf:hlm:M:N:nO:prRsv")) !=
-1)
```

**Inconsistent Implementations\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=202 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/scp.c | freebsd-src-2/scp.c |
| Line | 508 | 508 |
| Object | getopt | getopt |

Code Snippet
File Name freebsd-src-2/scp.c
Method main(int argc, char **argv)

```
....
508.        while ((ch = getopt(argc, argv,
```

**Inconsistent Implementations\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=203 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/valectl.c | freebsd-src-2/valectl.c |
| Line | 375 | 375 |
| Object | getopt | getopt |

Code Snippet
File Name freebsd-src-2/valectl.c
Method main(int argc, char *argv[])

```
....
375.        while ((ch = getopt(argc, argv, "d:a:h:g:l:n:r:C:p:P:m:v"))
!= -1) {
```

**Inconsistent Implementations\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=204 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/zinject.c | freebsd-src-2/zinject.c |
| Line | 792 | 792 |
| Object | getopt | getopt |

Code Snippet
File Name freebsd-src-2/zinject.c
Method main(int argc, char **argv)

```
....
792.         while ((c = getopt(argc, argv,
```

**Inconsistent Implementations\Path 6:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=205
Status New

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/diff.c | freebsd-src-2/diff.c |
| Line | 146 | 146 |
| Object | getopt_long | getopt_long |

Code Snippet
File Name freebsd-src-2/diff.c
Method main(int argc, char **argv)

```
....
146.         while ((ch = getopt_long(argc, argv, OPTIONS, longopts,
NULL)) != -1) {
```

## Privacy Violation

Query Path:
CPP\Cx\CPP Low Visibility\Privacy Violation Version:1

### Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

*Description*

**Privacy Violation\Path 1:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1158 |
| Status | New |

Method get_refdir at line 3656 of freebsd-src-2/test_main.c sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3731 | 4160 |
| Object | pwd | printf |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3731.        if (memcmp(pwd, "/usr/obj", 8) == 0) {
```

File Name freebsd-src-2/test_main.c
Method main(int argc, char **argv)

```
....
4160.              printf("Reference files will be read from: %s\n",
refdir);
```

**Privacy Violation\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1159 |
| Status | New |

Method get_refdir at line 3656 of freebsd-src-2/test_main.c sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3698 | 4160 |
| Object | pwd | printf |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3698.              pwd[strlen(pwd) - 1] = '\0';
```

File Name freebsd-src-2/test_main.c

Method main(int argc, char **argv)

```
....
4160.             printf("Reference files will be read from: %s\n",
refdir);
```

**Privacy Violation\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1160 |
| Status | New |

Method get_refdir at line 3656 of freebsd-src-2/test_main.c sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3693 | 4160 |
| Object | pwd | printf |

Code Snippet

File Name freebsd-src-2/test_main.c

Method get_refdir(const char *d)

```
....
3693.       pwd = getcwd(NULL, PATH_MAX);/* Solaris getcwd needs the
size. */
```

File Name freebsd-src-2/test_main.c

Method main(int argc, char **argv)

```
....
4160.             printf("Reference files will be read from: %s\n",
refdir);
```

**Privacy Violation\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1161 |
| Status | New |

Method get_refdir at line 3656 of freebsd-src-2/test_main.c sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3731 | 3747 |
| Object | pwd | printf |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3731.        if (memcmp(pwd, "/usr/obj", 8) == 0) {
....
3747.        printf("  Checked following directories:\n%s\n", tried);
```

**Privacy Violation\Path 5:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1162
Status New

Method get_refdir at line 3656 of freebsd-src-2/test_main.c sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3693 | 3747 |
| Object | pwd | printf |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3693.        pwd = getcwd(NULL, PATH_MAX);/* Solaris getcwd needs the
size. */
....
3747.        printf("  Checked following directories:\n%s\n", tried);
```

**Privacy Violation\Path 6:**

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=1163
Status New

Method get_refdir at line 3656 of freebsd-src-2/test_main.c sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/test_main.c | freebsd-src-2/test_main.c |
| Line | 3698 | 3747 |
| Object | pwd | printf |

Code Snippet
File Name freebsd-src-2/test_main.c
Method get_refdir(const char *d)

```
....
3698.              pwd[strlen(pwd) - 1] = '\0';
....
3747.        printf("  Checked following directories:\n%s\n", tried);
```

## 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=1060098&projectid=60088&pathid=423 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 696 | 696 |
| Object | > | > |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method int64_t X86_64::getImplicitAddend(const uint8_t *buf, RelType type) const {

```
....
696.      return SignExtend64<8>(*buf);
```

**Arithmenic Operation On Boolean\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=424 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 699 | 699 |
| Object | > | > |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method int64_t X86_64::getImplicitAddend(const uint8_t *buf, RelType type) const {

```
....
699.      return SignExtend64<16>(read16le(buf));
```

**Arithmenic Operation On Boolean\Path 3:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=425 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/X86_64.cpp | freebsd-src-2/X86_64.cpp |
| Line | 716 | 716 |
| Object | > | > |

Code Snippet
File Name freebsd-src-2/X86_64.cpp
Method int64_t X86_64::getImplicitAddend(const uint8_t *buf, RelType type) const {

```
....
716.      return SignExtend64<32>(read32le(buf));
```

**Arithmenic Operation On Boolean\Path 4:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=426 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/nsutils.c | freebsd-src-2/nsutils.c |
| Line | 685 | 685 |
| Object | BinaryExpr | BinaryExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/nsutils.c |
| Method | AcpiNsExternalizeName ( |

```
....
685.      RequiredLength = PrefixLength + (4 * NumSegments) +
```

## 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=1060098&projectid=60088&pathid=210 |
| Status | New |

The buffer allocated by <= in freebsd-src-2/ext2_extents.c at line 575 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-2/ext2_extents.c | freebsd-src-2/ext2_extents.c |
| Line | 583 | 583 |
| Object | <= | <= |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/ext2_extents.c |
| Method | ext4_ext_drop_refs(struct ext4_extent_path *path) |

```
....
583.        for (i = 0; i <= depth; i++, path++)
```

**Potential Off by One Error in Loops\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=211 |
| Status | New |

The buffer allocated by <= in freebsd-src-2/init.c at line 446 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-2/init.c | freebsd-src-2/init.c |
| Line | 497 | 497 |
| Object | <= | <= |

Code Snippet
File Name freebsd-src-2/init.c
Method int mt7615_register_ext_phy(struct mt7615_dev *dev)

```
....
497.         for (i = 0; i <= MT_TXQ_PSD ; i++)
```

**Potential Off by One Error in Loops\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=212 |
| Status | New |

The buffer allocated by <= in freebsd-src-2/sh.glob.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-2/sh.glob.c | freebsd-src-2/sh.glob.c |
| Line | 185 | 185 |
| Object | <= | <= |

Code Snippet
File Name freebsd-src-2/sh.glob.c
Method globbrace(const Char *s, Char ***bl)

```
....
185.       for (i = 0, pl = pm = p; pm <= pe; pm++)
```

## Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read Version:0

### Categories

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

*Description*

**Heuristic 2nd Order Buffer Overflow read\Path 1:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=393 |
| Status | New |

The size of the buffer used by evbuffer_file_segment_materialize in BinaryExpr, at line 3027 of freebsd-src-2/buffer.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that evbuffer_file_segment_materialize passes to BinaryExpr, at line 3027 of freebsd-src-2/buffer.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 3107 | 3107 |
| Object | BinaryExpr | BinaryExpr |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_file_segment_materialize(struct evbuffer_file_segment *seg)

```
....
3107.                    n = read(fd, mem+read_so_far, length-
read_so_far);
```

**Heuristic 2nd Order Buffer Overflow read\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=394 |
| Status | New |

The size of the buffer used by evbuffer_file_segment_materialize in length, at line 3027 of freebsd-src-2/buffer.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that evbuffer_file_segment_materialize passes to BinaryExpr, at line 3027 of freebsd-src-2/buffer.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 3107 | 3107 |
| Object | BinaryExpr | length |

Code Snippet
File Name freebsd-src-2/buffer.c
Method evbuffer_file_segment_materialize(struct evbuffer_file_segment *seg)

```
....
3107.                    n = read(fd, mem+read_so_far, length-
read_so_far);
```

**Heuristic 2nd Order Buffer Overflow read\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=395 |
| Status | New |

The size of the buffer used by evbuffer_file_segment_materialize in read_so_far, at line 3027 of freebsd-src-2/buffer.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that evbuffer_file_segment_materialize passes to BinaryExpr, at line 3027 of freebsd-src-2/buffer.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/buffer.c | freebsd-src-2/buffer.c |
| Line | 3107 | 3107 |
| Object | BinaryExpr | read_so_far |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/buffer.c |
| Method | evbuffer_file_segment_materialize(struct evbuffer_file_segment *seg) |

```
....
3107.                    n = read(fd, mem+read_so_far, length-
read_so_far);
```

## 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=1060098&projectid=60088&pathid=396 |
| Status | New |

The size of the buffer used by make_rsid in "%s:%s", at line 656 of freebsd-src-2/rtsol.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that make_rsid passes to "%s:%s", at line 656 of freebsd-src-2/rtsol.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 661 | 661 |
| Object | "%s:%s" | "%s:%s" |

| | |
|---|---|
| Code Snippet | |
| File Name | freebsd-src-2/rtsol.c |
| Method | make_rsid(const char *ifname, const char *origin, struct rainfo *rai) |

```
....
661.                sprintf(rsid, "%s:%s", ifname, origin);
```

**Potential Precision Problem\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060098&projectid=60088&pathid=397 |
| Status | New |

The size of the buffer used by make_rsid in "%s:%s:[%s]", at line 656 of freebsd-src-2/rtsol.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that make_rsid passes to "%s:%s:[%s]", at line 656 of freebsd-src-2/rtsol.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |
| Line | 669 | 669 |
| Object | "%s:%s:[%s]" | "%s:%s:[%s]" |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method make_rsid(const char *ifname, const char *origin, struct rainfo *rai)

```
....
669.                sprintf(rsid, "%s:%s:[%s]", ifname, origin, hbuf);
```

## 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=1060098&projectid=60088&pathid=1318 |
| Status | New |

The make_rsid method performs a reverse DNS lookup with getnameinfo, at line 656 of freebsd-src-2/rtsol.c. The application then makes a security decision, !=, in freebsd-src-2/rtsol.c line 656, even though this hostname is not reliable and can be easily spoofed.

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/rtsol.c | freebsd-src-2/rtsol.c |

| | | |
|---|---|---|
| Line | 665 | 667 |
| Object | getnameinfo | != |

Code Snippet
File Name freebsd-src-2/rtsol.c
Method make_rsid(const char *ifname, const char *origin, struct rainfo *rai)

```
....
665.                if (getnameinfo((struct sockaddr *)&rai->rai_saddr,
....
667.                        NI_NUMERICHOST) != 0)
```

## 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=1060098&projectid=60088&pathid=1532 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/session.c | freebsd-src-2/session.c |
| Line | 269 | 269 |
| Object | mkstemp | mkstemp |

Code Snippet
File Name freebsd-src-2/session.c
Method prepare_auth_info_file(struct passwd *pw, struct sshbuf *info)

```
....
269.        if ((fd = mkstemp(auth_info_file)) == -1) {
```

## 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=1060098&projectid=60088&pathid=1600 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | freebsd-src-2/statem_srvr.c | freebsd-src-2/statem_srvr.c |
| Line | 1743 | 1743 |
| Object | cipher- | cipher- |

Code Snippet
File Name freebsd-src-2/statem_srvr.c
Method /* Check what signalling cipher-suite values were received. */

```
....
1743.      /* Check what signalling cipher-suite values were received.
*/
```

# 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));
    }
}
```

# Off by One Error in Arrays

## 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

# 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

# CGI Stored XSS

## Risk

**What might happen**

Stored malicious data might retrieve system information and exploit the system through CGI (Common Gateway Interface).

---

## Cause

**How does it happen**

The CGI specification provides opportunities to read files, acquire shell access, and corrupt file systems on server machines and their attached hosts.

Means of gaining access include: exploiting assumptions of the script, exploiting weaknesses in the server environment, and exploiting weaknesses in other programs and system calls.

The primary weakness in CGI scripts is insufficient input validation.

---

## General Recommendations

**How to avoid it**

Do not provide unnecessary file permissions.

Validate and encode all DB output.

---

## Source Code Examples

**Perl**

**Bad - Printing out data from BD without encoding**

```
#!/usr/bin/perl
use CGI;
use DBI;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", @row),
      $cgi->end_html;
```

### Good - Printing out from DB after encoding

```
#!/usr/bin/perl
use CGI;
use DBI;
use HTML::Entities;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", HTML::Entities::encode(@row)),
      $cgi->end_html;
```

# Buffer Overflow AddressOfLocalVarReturned

## Risk

### What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

---

## Cause

### How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

---

## General Recommendations

### How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

## Source Code Examples

### CPP

**Use of Variable after It was Freed**

```
free(input);
printf("%s", input);
```

**Use of Pointer to Local Variable That Was Freed On Return**

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

# Buffer Overflow boundcpy WrongSizeParam

## Risk

### What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

---

## Cause

### How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

---

## General Recommendations

### How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

---

## Source Code Examples

# 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;
}
```

# Divide By Zero

## Risk

### What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

## Cause

### How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

## General Recommendations

### How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

## Source Code Examples

### Java

**Divide by Zero**

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

**Checked Division**

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

# MemoryFree on StackVariable

## Risk

**What might happen**

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

---

## Cause

**How does it happen**

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

---

## General Recommendations

**How to avoid it**

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

---

## Source Code Examples

**CPP**

**Bad - Calling free() on a static variable**

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

**Good - Calling free() only on variables that were dynamically allocated**

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

# Wrong Size t Allocation

## Risk

### What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

## Cause

### How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

## General Recommendations

### How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

## Source Code Examples

### CPP

**Allocating and Assigning Memory without Sizeof Arithmetic**

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

**Allocating and Assigning Memory with Sizeof Arithmetic**

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

### Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

### Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

# Integer Overflow

## Risk

### What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

---

## Cause

### How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

---

## General Recommendations

### How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

## Source Code Examples

# Dangerous Functions

## Risk

### What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

---

## Cause

### How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

---

## General Recommendations

### How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

---

## Source Code Examples

### CPP

### Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

### Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

### Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

### Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

### Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

### Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

## 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<br>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

# 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();
        }
    }
}
```

# 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

## Use of Uninitialized Variable

**Weakness ID:** 457 *(Weakness Variant)* **Status:** Draft

### Description

### Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

### Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

### Time of Introduction

- Implementation

### Applicable Platforms

### Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

### Common Consequences

| Scope | Effect |
|---|---|
| Availability<br>Integrity | Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not. |
| Authorization | Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string. |

### Likelihood of Exploit

High

### Demonstrative Examples

### Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

*(Bad Code)*

*Example Language:* **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

## Example 2

*Example Languages:* **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

### Observed Examples

| Reference | Description |
|---|---|
| CVE-2008-0081 | Uninitialized variable leads to code execution in popular desktop application. |
| CVE-2007-4682 | Crafted input triggers dereference of an uninitialized object pointer. |
| CVE-2007-3468 | Crafted audio file triggers crash when an uninitialized variable is used. |
| CVE-2007-2728 | Uninitialized random seed variable used. |

### Potential Mitigations

**Phase: Implementation**

Assign all variables to an initial value.

**Phase: Build and Compilation**

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

**Phase: Requirements**

The choice could be made to use a language that is not susceptible to these issues.

**Phase: Architecture and Design**

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

### Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

### Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---|---|---|---|---|
| ChildOf | Weakness Class | 398 | Indicator of Poor Code Quality | **Seven Pernicious Kingdoms (primary)700** |
| ChildOf | Weakness Base | 456 | Missing Initialization | **Development Concepts (primary)699 Research Concepts** |

| | | | | |
|---|---|---|---|---|
| | | | | **(primary)1000** |
| MemberOf | View | 630 | Weaknesses Examined by SAMATE | **Weaknesses Examined by SAMATE (primary)630** |

## Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|---|---|---|---|
| CLASP | | | Uninitialized variable |
| 7 Pernicious Kingdoms | | | Uninitialized Variable |

## White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

## References


mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.


## Content History

**Submissions**

| Submission Date | Submitter | Organization | Source |
|---|---|---|---|
| | CLASP | | Externally Mined |

**Modifications**

| Modification Date | Modifier | Organization | Source |
|---|---|---|---|
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings | | |
| 2009-01-12 | CWE Content Team | MITRE | Internal |
| | updated Common Consequences, Demonstrative Examples, Potential Mitigations | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2009-05-27 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |

**Previous Entry Names**

| Change Date | Previous Entry Name |
|---|---|
| 2008-04-11 | Uninitialized Variable |

BACK TO TOP

# Use of Zero Initialized Pointer

## Risk

### What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

---

## Cause

### How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

---

## General Recommendations

### How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

---

## Source Code Examples

### CPP

**Explicit NULL Dereference**

```
char * input = NULL;
printf("%s", input);
```

**Implicit NULL Dereference**

```
char * input;
printf("%s", input);
```

### Java

**Explicit Null Dereference**

```
Object o = null;
out.println(o.getClass());
```

## Use of Function with Inconsistent Implementations

**Weakness ID:** 474 *(Weakness Base)* **Status:** Draft

### Description

## Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

### Time of Introduction

- Architecture and Design
- Implementation

### Applicable Platforms

## Languages

C: *(Often)*

PHP: *(Often)*

All

### Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

### Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

### Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---|---|---|---|---|
| ChildOf | Weakness Class | 398 | Indicator of Poor Code Quality | **Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000** |
| ParentOf | Weakness Variant | 589 | Call to Non-ubiquitous API | **Research Concepts (primary)1000** |

### Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|---|---|---|---|
| 7 Pernicious Kingdoms | | | Inconsistent Implementations |

### Content History

| Submissions | | | |
|---|---|---|---|
| **Submission Date** | **Submitter** | **Organization** | **Source** |
| | 7 Pernicious Kingdoms | | Externally Mined |
| **Modifications** | | | |
| **Modification Date** | **Modifier** | **Organization** | **Source** |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Potential Mitigations, Time of Introduction | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings | | |
| **Previous Entry Names** | | | |
| **Change Date** | **Previous Entry Name** | | |
| 2008-04-11 | Inconsistent Implementations | | |

BACK TO TOP

# Potential Off by One Error in Loops

## Risk

### What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

---

## Cause

### How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

---

## General Recommendations

### How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

---

## Source Code Examples

### CPP

### Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

### Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

### Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

# Heuristic 2nd Order Buffer Overflow read

## Risk

### What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

---

## Cause

### How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

---

## General Recommendations

### How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

---

## Source Code Examples

# 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

## 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 {
    //[..]
};
```

# Privacy Violation

## Risk

### What might happen

A user’s personal information could be stolen by a malicious programmer, or an attacker that intercepts the data.

---

## Cause

### How does it happen

The application sends user information, such as passwords, account information, or credit card numbers, outside the application, such as writing it to a local text or log file or sending it to an external web service.

---

## General Recommendations

### How to avoid it

1. Personal data should be removed before writing to logs or other files.
2. Review the need and justification of sending personal data to remote web services.

---

## Source Code Examples

### CSharp

#### The user's password is written to the screen

```
class PrivacyViolation
{
        static void foo(string insert_sql)
    {

                string password = "unsafe_password";
                insert_sql = insert_sql.Replace("$password", password);
                System.Console.WriteLine(insert_sql);
        }
}
```

#### the user's password is MD5 coded before being written to the screen

```
class PrivacyViolationFixed
{
        static void foo(string insert_sql)
    {
```

```
                string password = "unsafe_password";
                MD5 md5Hash = System.Security.Cryptography.MD5.Create();
                byte[] data = md5Hash.ComputeHash(Encoding.UTF8.GetBytes(password));
        StringBuilder md5Password = new StringBuilder();

                for (int i = 0; i < data.Length; i++)
            {
                   md5Password.Append(data[i].ToString("x2"));
            }
            insert_sql = insert_sql.Replace("$password", md5Password.ToString());
                System.Console.WriteLine(insert_sql);
        }
}
```

# 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

# 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

# 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 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<br>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<br>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<br>Availability<br>Confidentiality | A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution. |

### Likelihood of Exploit

High

### Detection Methods

**Automated Static Analysis**

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

## *Effectiveness: High*

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

**Automated Dynamic Analysis**

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

**Black Box**

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

## Demonstrative Examples

### Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

*(Bad Code)*

*Example Language:* **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

*(Good Code)*

*Example Language:* **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

## Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

*(Bad Code)*

*Example Language:* **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

## Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

*(Bad Code)*

*Example Language:* **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

*(Good Code)*

*Example Language:* **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

*(Good Code)*

*Example Language:* **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

## Observed Examples

| Reference | Description |
|---|---|
| CVE-2005-0369 | large ID in packet used as array index |
| CVE-2001-1009 | negative array index as argument to POP LIST command |
| CVE-2003-0721 | Integer signedness error leads to negative array index |
| CVE-2004-1189 | product does not properly track a count and a maximum number, which can lead to resultant array index overflow. |
| CVE-2007-5756 | chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error. |

## Potential Mitigations

**Phase: Architecture and Design**

### Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

**Phase: Architecture and Design**

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

**Phase: Requirements**

### Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

**Phase: Implementation**

## Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

**Phase: Implementation**

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

### Weakness Ordinalities

| Ordinality | Description |
|---|---|
| Resultant | The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer. |

### Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---|---|---|---|---|
| ChildOf | Weakness Class | 20 | Improper Input Validation | **Development Concepts (primary)699 Research Concepts (primary)1000** |
| ChildOf | Category | 189 | Numeric Errors | Development Concepts699 |
| ChildOf | Category | 633 | Weaknesses that Affect Memory | **Resource-specific Weaknesses (primary)631** |
| ChildOf | Category | 738 | CERT C Secure Coding Section 04 - Integers (INT) | **Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734** |
| ChildOf | Category | 740 | CERT C Secure Coding Section 06 - Arrays (ARR) | Weaknesses Addressed by the CERT C Secure Coding Standard734 |
| ChildOf | Category | 802 | 2010 Top 25 - Risky Resource Management | **Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800** |
| CanPrecede | Weakness Class | 119 | Failure to Constrain Operations within the Bounds of a Memory Buffer | Research Concepts1000 |
| CanPrecede | Weakness Variant | 789 | Uncontrolled Memory Allocation | Research Concepts1000 |
| PeerOf | Weakness Base | 124 | Buffer Underwrite ('Buffer Underflow') | Research Concepts1000 |

### Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

### Affected Resources

- Memory

### f Causal Nature

Explicit

### Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|---|---|---|---|
| CLASP | | | Unchecked array indexing |
| PLOVER | | | INDEX - Array index overflow |
| CERT C Secure Coding | ARR00-C | | Understand how arrays work |
| CERT C Secure Coding | ARR30-C | | Guarantee that array indices are within the valid range |
| CERT C Secure Coding | ARR38-C | | Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element |
| CERT C Secure Coding | INT32-C | | Ensure that operations on signed integers do not result in overflow |

### Related Attack Patterns

| CAPEC-ID | Attack Pattern Name | *(CAPEC Version: 1.5)* |
|---|---|---|
| 100 | Overflow Buffers | |

### References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

### Content History

| Submissions | | | |
|---|---|---|---|
| **Submission Date** | **Submitter** | **Organization** | **Source** |
| | CLASP | | Externally Mined |
| **Modifications** | | | |
| **Modification Date** | **Modifier** | **Organization** | **Source** |
| 2008-07-01 | Sean Eidemiller | Cigital | External |
| | added/updated demonstrative examples | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities | | |
| 2008-11-24 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Taxonomy Mappings | | |
| 2009-01-12 | CWE Content Team | MITRE | Internal |
| | updated Common Consequences | | |
| 2009-10-29 | CWE Content Team | MITRE | Internal |
| | updated Description, Name, Relationships | | |
| 2009-12-28 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships | | |
| 2010-04-05 | CWE Content Team | MITRE | Internal |
| | updated Related Attack Patterns | | |
| **Previous Entry Names** | | | |
| **Change Date** | **Previous Entry Name** | | |
| 2009-10-29 | Unchecked Array Indexing | | |

BACK TO TOP

# TOCTOU

## Risk

### What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

---

## Cause

### How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

---

## General Recommendations

### How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

---

## Source Code Examples

### Java

**Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition**

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

**Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition**

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

## Information Leak Through Comments

**Weakness ID:** 615 *(Weakness Variant)* **Status:** Incomplete

### Description

## Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

## Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

### Time of Introduction

- Implementation

### Demonstrative Examples

## Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

*(Bad Code)*

*Example Languages:* **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

### Observed Examples

| Reference | Description |
|---|---|
| CVE-2007-6197 | Version numbers and internal hostnames leaked in HTML comments. |
| CVE-2007-4072 | CMS places full pathname of server in HTML comment. |
| CVE-2009-2431 | blog software leaks real username in HTML comment. |

### Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

### Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---|---|---|---|---|
| ChildOf | Weakness Variant | 540 | Information Leak Through Source Code | **Development Concepts (primary)699 Research Concepts (primary)1000** |

### Content History

| Submissions | | | |
|---|---|---|---|
| **Submission Date** | **Submitter** | **Organization** | **Source** |
| | Anonymous Tool Vendor (under NDA) | | Externally Mined |
| **Modifications** | | | |
| **Modification Date** | **Modifier** | **Organization** | **Source** |
| 2008-07-01 | Sean Eidemiller | Cigital | External |
| | added/updated demonstrative examples | | |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Potential Mitigations, Time of Introduction | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Taxonomy Mappings | | |
| 2008-10-14 | CWE Content Team | MITRE | Internal |
| | updated Description | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |

| | | | |
|---|---|---|---|
| | updated Demonstrative Examples | | |
| 2009-07-27 | CWE Content Team | MITRE | Internal |
| | updated Observed Examples, Taxonomy Mappings | | |

BACK TO TOP

## Scanned Languages

| Language | Hash Number | Change Date |
|---|---|---|
| CPP | 4541647240435660 | 6/19/2024 |
| Common | 0105849645654507 | 6/19/2024 |