AdAway Scan Report

Project Name	AdAway
Scan Start	Thursday, June 20, 2024 9:29:59 AM
Preset	Checkmarx Default
Scan Time	01h:37m:56s
Lines Of Code Scanned	175610
Files Scanned	412
Report Creation Time	Thursday, June 20, 2024 10:11:20 AM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	9/1000 (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

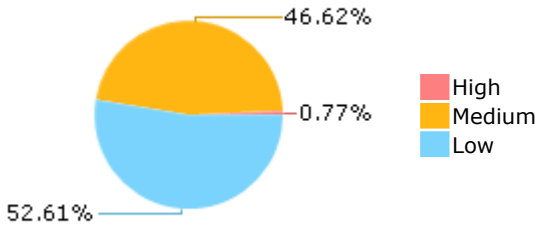
Results Limit

Results limit per query was set to 50

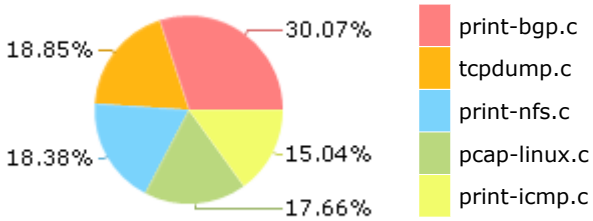
Selected Queries

Selected queries are listed in Result Summary

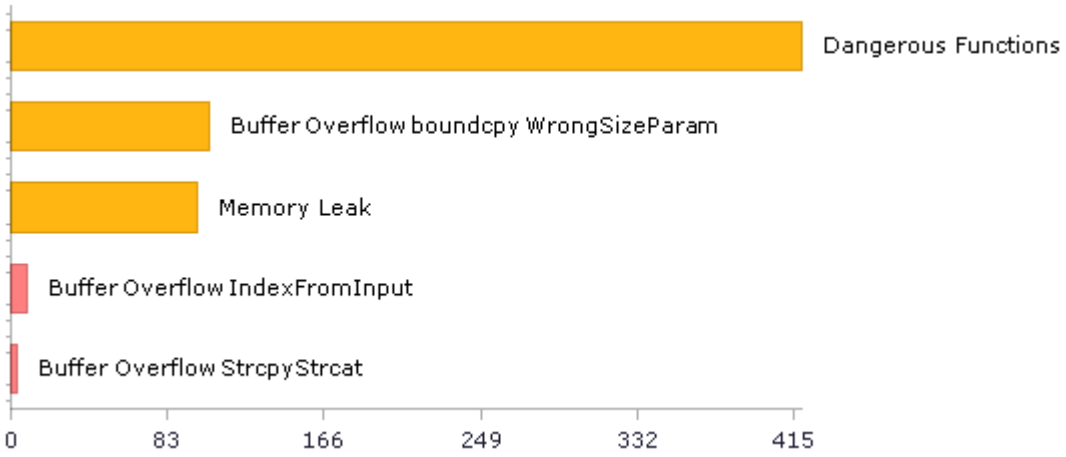
Result Summary



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	193	146
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	182	182
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	8	4
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	5	2
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)*	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	420	420
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)*	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References*	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	5	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	2	1
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	420	420
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	4	4
PCI DSS (3.2) - 6.5.2 - Buffer overflows	128	128
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery*	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	15	15
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	1	1
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	34	20
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.	174	170
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.	1	1
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.	13	13

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	209	198
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)	7	4
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	5	2
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	2	1
SC-5 Denial of Service Protection (P1)*	187	129
SC-8 Transmission Confidentiality and Integrity (P1)	1	1
SI-10 Information Input Validation (P1)*	60	55
SI-11 Error Handling (P2)*	129	129
SI-15 Information Output Filtering (P0)*	0	0
SI-16 Memory Protection (P1)	7	7

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

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage*	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality*	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering*	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

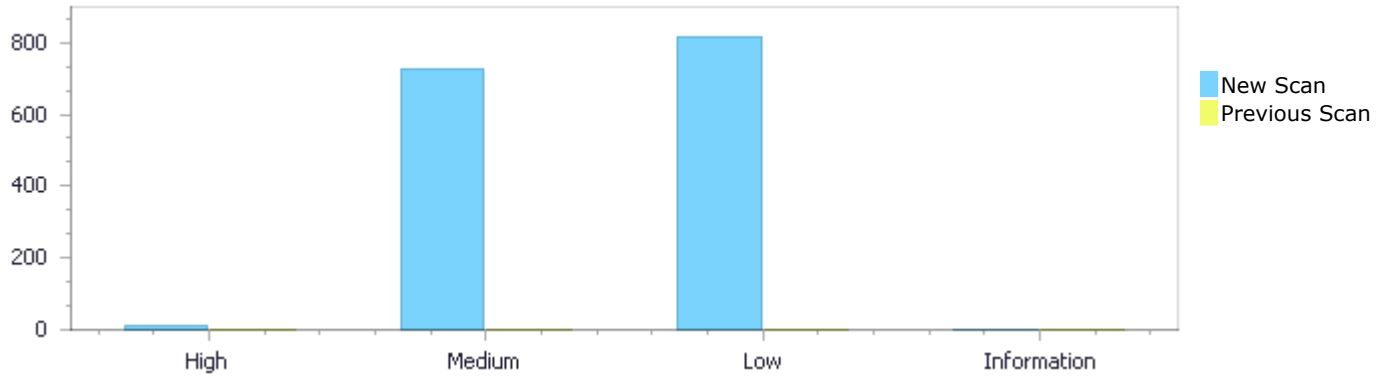
***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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	12	724	817	0	1,553
Recurrent Issues	0	0	0	0	0
Total	12	724	817	0	1,553
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	12	724	817	0	1,553
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	12	724	817	0	1,553

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	9	High
Buffer Overflow StrcpyStrcat	3	High
Dangerous Functions	419	Medium
Buffer Overflow boundcpy WrongSizeParam	105	Medium
Memory Leak	99	Medium

Use of Zero Initialized Pointer	29	Medium
MemoryFree on StackVariable	19	Medium
Wrong Size t Allocation	12	Medium
Integer Overflow	7	Medium
Stored Buffer Overflow boundcpy	7	Medium
Inadequate Encryption Strength	6	Medium
Buffer Overflow AddressOfLocalVarReturned	4	Medium
Short Overflow	4	Medium
Char Overflow	2	Medium
Divide By Zero	2	Medium
Double Free	2	Medium
Wrong Memory Allocation	2	Medium
Client Use Of JQuery Outdated Version	1	Medium
Client Use Of JQuery Outdated Version	1	Medium
Off by One Error in Methods	1	Medium
Use of a One Way Hash without a Salt	1	Medium
Use of Uninitialized Variable	1	Medium
Use of Sizeof On a Pointer Type	259	Low
Improper Resource Access Authorization	167	Low
Unchecked Return Value	129	Low
Sizeof Pointer Argument	78	Low
NULL Pointer Dereference	53	Low
TOCTOU	31	Low
Exposure of System Data to Unauthorized Control Sphere	27	Low
Unchecked Array Index	26	Low
Incorrect Permission Assignment For Critical Resources	15	Low
Potential Path Traversal	5	Low
Potential Precision Problem	5	Low
Reliance on DNS Lookups in a Decision	5	Low
Potential Off by One Error in Loops	4	Low
Inconsistent Implementations	3	Low
Heuristic 2nd Order Buffer Overflow malloc	2	Low
Privacy Violation	2	Low
Unsafe Use Of Target blank	2	Low
Unsafe Use Of Target blank	2	Low
Arithmenic Operation On Boolean	1	Low
Client Insufficient ClickJacking Protection	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
tcpdump/jni/tcpdump/print-bgp.c	62
tcpdump/jni/tcpdump/addrtoname.c	45
tcpdump/jni/libpcap/pcap-linux.c	42
tcpdump/jni/tcpdump/print-icmp.c	35
tcpdump/jni/libpcap/optimize.c	29
tcpdump/jni/libpcap/inet.c	29
tcpdump/jni/libpcap/pcap-bpf.c	27
tcpdump/jni/libpcap/pcap-usb-linux.c	18

tcpdump/jni/libpcap/fad-gifc.c	17
tcpdump/jni/tcpdump/print-esp.c	17

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1
Status	New

The size of the buffer used by yy_get_next_buffer in Address, at line 3986 of tcpdump/jni/libpcap/scanner.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that yy_get_next_buffer passes to getc, at line 3986 of tcpdump/jni/libpcap/scanner.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4076	4076
Object	getc	Address

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static int yy_get_next_buffer (void)

```
....
4076.             YY_INPUT( (&YY_CURRENT_BUFFER_LVALUE-
>yy_ch_buf[number_to_move]),
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=2
Status	New

The size of the buffer used by yy_get_next_buffer in Address, at line 3986 of tcpdump/jni/libpcap/scanner.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that yy_get_next_buffer passes to getc, at line 3986 of tcpdump/jni/libpcap/scanner.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c

Line	4076	4076
Object	getc	Address

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static int yy_get_next_buffer (void)

```
....
4076.             YY_INPUT( (&YY_CURRENT_BUFFER_LVALUE-
>yy_ch_buf[number_to_move]),
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=3
Status	New

The size of the buffer used by YY_DECL in yy_buffer_stack, at line 2954 of tcpdump/jni/libpcap/scanner.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that YY_DECL passes to stdin, at line 2954 of tcpdump/jni/libpcap/scanner.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	2976	3871
Object	stdin	yy_buffer_stack

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method YY_DECL

```
....
2976.                   pcap_in = stdin;
....
3871.                   YY_CURRENT_BUFFER_LVALUE->yy_input_file =
pcap_in;
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=4
Status	New

The size of the buffer used by ataddr_string in BinaryExpr, at line 536 of tcpdump/jni/tcpdump/print-atalk.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ataddr_string passes to line, at line 536 of tcpdump/jni/tcpdump/print-atalk.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	554	566
Object	line	BinaryExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
554.                while (fgets(line, sizeof(line), fp)) {
....
566.                        for (tp = &hnametable[i2 & (HASHNAMESIZE-1)];
```

Buffer Overflow IndexFromInput\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=5
Status New

The size of the buffer used by usb_read_linux in ret, at line 468 of tcpdump/jni/libpcap/pcap-usb-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that usb_read_linux passes to line, at line 468 of tcpdump/jni/libpcap/pcap-usb-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	487	506
Object	line	ret

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_read_linux(pcap_t *handle, int max_packets, pcap_handler callback, u_char *user)

```
....
487.                ret = read(handle->fd, line, USB_LINE_LEN - 1);
....
506.        string[ret] = 0;
```

Buffer Overflow IndexFromInput\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=6
Status New

The size of the buffer used by usb_stats_linux in ret, at line 674 of tcpdump/jni/libpcap/pcap-usb-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that usb_stats_linux passes to string, at line 674 of tcpdump/jni/libpcap/pcap-usb-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	706	716
Object	string	ret

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_stats_linux(pcap_t *handle, struct pcap_stat *stats)

```
....
706.              ret = read(fd, string, USB_LINE_LEN-1);
....
716.        string[ret] = 0;
```

Buffer Overflow IndexFromInput\Path 7:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=7
Status New

The size of the buffer used by read_infile in cc, at line 75 of tcpdump/jni/libpcap/tests/filtertest.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_infile passes to cp, at line 75 of tcpdump/jni/libpcap/tests/filtertest.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/tests/filtertest.c	tcpdump/jni/libpcap/tests/filtertest.c
Line	92	105
Object	cp	cc

Code Snippet
File Name tcpdump/jni/libpcap/tests/filtertest.c
Method read_infile(char *fname)

```
....
92.   cc = read(fd, cp, (u_int)buf.st_size);
....
105.        cp[cc] = '\0';
```

Buffer Overflow IndexFromInput\Path 8:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=8
Status	New

The size of the buffer used by read_infile in cc, at line 103 of tcpdump/jni/libpcap/tests/valgrindtest.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_infile passes to cp, at line 103 of tcpdump/jni/libpcap/tests/valgrindtest.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/tests/valgrindtest.c	tcpdump/jni/libpcap/tests/valgrindtest.c
Line	120	133
Object	cp	cc

Code Snippet
File Name tcpdump/jni/libpcap/tests/valgrindtest.c
Method read_infile(char *fname)

```
....
120.        cc = read(fd, cp, (u_int)buf.st_size);
....
133.        cp[cc] = '\0';
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=9
Status	New

The size of the buffer used by get_mac80211_phydev in bytes_read, at line 545 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_mac80211_phydev passes to phydev_path, at line 545 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	560	577
Object	phydev_path	bytes_read

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method get_mac80211_phydev(pcap_t *handle, const char *device, char *phydev_path,

```
....
560.        bytes_read = readlink(pathstr, phydev_path,
phydev_max_pathlen);
....
577.        phydev_path[bytes_read] = '\0';
```

Buffer Overflow StrcpyStrcat

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=10
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in errbuf, at line 38 of tcpdump/jni/libpcap/fad-sita.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to errbuf, at line 38 of tcpdump/jni/libpcap/fad-sita.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-sita.c	tcpdump/jni/libpcap/fad-sita.c
Line	38	43
Object	errbuf	errbuf

Code Snippet
File Name tcpdump/jni/libpcap/fad-sita.c
Method int pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf) {

```
....
38.  int pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)
{
....
43.   strcpy(errbuf, "");
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=11
Status	New

The size of the buffer used by inet_ntop_v6 in dst, at line 99 of tcpdump/jni/tcpdump/missing/inet_ntop.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that inet_ntop_v6 passes to dst, at line 99 of tcpdump/jni/tcpdump/missing/inet_ntop.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/missing/inet_ntop.c	tcpdump/jni/tcpdump/missing/inet_ntop.c

Line	99	197
Object	dst	dst

Code Snippet
File Name tcpdump/jni/tcpdump/missing/inet_ntop.c
Method inet_ntop_v6 (const u_char *src, char *dst, size_t size)

```
....
99.  inet_ntop_v6 (const u_char *src, char *dst, size_t size)
....
197.    return strcpy (dst, tmp);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=12
Status	New

The size of the buffer used by ether_ntohost in name, at line 202 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ether_ntohost passes to name, at line 202 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	202	214
Object	name	name

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method int ether_ntohost (char *name, struct ether_addr *e)

```
....
202.  int ether_ntohost (char *name, struct ether_addr *e)
....
214.          strcpy (name,cache->name);
```

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=1000001&projectid=2&pathid=170
Status	New

The dangerous function, _snprintf, was found in use at line 1221 in tcpdump/jni/tcpdump/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	1224	1224
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method ieee8021q_tci_string(const uint16_t tci)

```
....
1224.       snprintf(buf, sizeof(buf), "vlan %u, p %u%s",
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=171
Status	New

The dangerous function, _snprintf, was found in use at line 470 in tcpdump/jni/tcpdump/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	508	508
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method etheraddr_string(netdissect_options *ndo, register const u_char *ep)

```
....
508.             snprintf(cp, BUFSIZE - (2 + 5*3), " (oui %s)",
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=172
Status	New

The dangerous function, _snprintf, was found in use at line 663 in tcpdump/jni/tcpdump/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	676	676
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method tcpport_string(u_short port)

```
....
676.         (void)snprintf(buf, sizeof(buf), "%u", i);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=173
Status	New

The dangerous function, _snprintf, was found in use at line 682 in tcpdump/jni/tcpdump/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	695	695
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method udpport_string(register u_short port)

```
....
695.         (void)snprintf(buf, sizeof(buf), "%u", i);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=174
Status	New

The dangerous function, _snprintf, was found in use at line 727 in tcpdump/jni/tcpdump/addrtoname.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	747	747
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method init_servarray(netdissect_options *ndo)

```
....
747.                    (void)snprintf(buf, sizeof(buf), "%d", port);
```

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=175
Status New

The dangerous function, _snprintf, was found in use at line 93 in tcpdump/jni/tcpdump/print-ascii.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-ascii.c	tcpdump/jni/tcpdump/print-ascii.c
Line	112	112
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-ascii.c
Method hex_and_ascii_print_with_offset(netdissect_options *ndo, register const char *ident,

```
....
112.                (void)snprintf(hsp, sizeof(hexstuff) - (hsp -
hexstuff),
```

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=176
Status New

The dangerous function, _snprintf, was found in use at line 93 in tcpdump/jni/tcpdump/print-ascii.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-ascii.c	tcpdump/jni/tcpdump/print-ascii.c
Line	129	129
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-ascii.c
Method hex_and_ascii_print_with_offset(netdissect_options *ndo, register const char *ident,

```
....
129.                (void)snprintf(hsp, sizeof(hexstuff) - (hsp -
hexstuff),
```

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=177
Status New

The dangerous function, _snprintf, was found in use at line 612 in tcpdump/jni/tcpdump/print-atalk.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	618	618
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ddpskt_string(netdissect_options *ndo,

```
....
618.                (void)snprintf(buf, sizeof(buf), "%d", skt);
```

Dangerous Functions\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=178
Status New

The dangerous function, _snprintf, was found in use at line 536 in tcpdump/jni/tcpdump/print-atalk.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	586	586
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
586.                    (void)snprintf(nambuf, sizeof(nambuf), "%s.%d",
```

Dangerous Functions\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=179
Status New

The dangerous function, _snprintf, was found in use at line 536 in tcpdump/jni/tcpdump/print-atalk.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	595	595
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
595.                (void)snprintf(nambuf, sizeof(nambuf), "%d.%d", atnet,
athost);
```

Dangerous Functions\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=180
Status New

The dangerous function, _snprintf, was found in use at line 536 in tcpdump/jni/tcpdump/print-atalk.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	597	597
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
597.                (void)snprintf(nambuf, sizeof(nambuf), "%d", atnet);
```

Dangerous Functions\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=181
Status New

The dangerous function, _snprintf, was found in use at line 107 in tcpdump/jni/tcpdump/print-babel.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	110	110
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_id(const u_char *id)

```
....
110.      snprintf(buf, 25, "%02x:%02x:%02x:%02x:%02x:%02x:%02x:%02x",
```

Dangerous Functions\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=182
Status New

The dangerous function, _snprintf, was found in use at line 120 in tcpdump/jni/tcpdump/print-babel.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c

Line	124	124
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_prefix(netdissect_options *ndo, const u_char *prefix, unsigned char plen)

```
....
124.          snprintf(buf, 50, "%s/%u", ipaddr_string(ndo, prefix +
12), plen - 96);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=183
Status	New

The dangerous function, _snprintf, was found in use at line 120 in tcpdump/jni/tcpdump/print-babel.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	127	127
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_prefix(netdissect_options *ndo, const u_char *prefix, unsigned char plen)

```
....
127.          snprintf(buf, 50, "%s/%u", ip6addr_string(ndo, prefix),
plen);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=184
Status	New

The dangerous function, _snprintf, was found in use at line 149 in tcpdump/jni/tcpdump/print-babel.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	155	155

Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_interval(const uint16_t i)

```
....
155.      snprintf(buf, sizeof(buf), "%u.%02us", i / 100, i % 100);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=185
Status	New

The dangerous function, _snprintf, was found in use at line 166 in tcpdump/jni/tcpdump/print-babel.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	169	169
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_timestamp(const uint32_t i)

```
....
169.      snprintf(buf, sizeof(buf), "%u.%06us", i / 1000000, i %
1000000);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=186
Status	New

The dangerous function, _snprintf, was found in use at line 470 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	474	474
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method as_printf(netdissect_options *ndo,

```
....
474.                snprintf(str, size, "%u", asnum);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=187
Status	New

The dangerous function, _snprintf, was found in use at line 470 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	476	476
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method as_printf(netdissect_options *ndo,

```
....
476.                snprintf(str, size, "%u.%u", asnum >> 16, asnum &
0xFFFF);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=188
Status	New

The dangerous function, _snprintf, was found in use at line 484 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	506	506
Object	_snprintf	_snprintf

Code Snippet

File Name	tcpdump/jni/tcpdump/print-bgp.c
Method	decode_prefix4(netdissect_options *ndo,

```
....
506.        snprintf(buf, buflen, "%s/%d", getname(ndo, (u_char
*)&addr), plen);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=189
Status	New

The dangerous function, _snprintf, was found in use at line 517 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	555	555
Object	_snprintf	_snprintf

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-bgp.c
Method	decode_labeled_prefix4(netdissect_options *ndo,

```
....
555.        snprintf(buf, buflen, "%s/%d, label:%u %s",
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=190
Status	New

The dangerous function, _snprintf, was found in use at line 576 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	587	587
Object	_snprintf	_snprintf

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-bgp.c
Method	bgp_vpn_ip_print(netdissect_options *ndo,

```
....
587.          snprintf(pos, sizeof(addr), "%s", ipaddr_string(ndo,
pptr));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=191
Status	New

The dangerous function, _snprintf, was found in use at line 576 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	592	592
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_ip_print(netdissect_options *ndo,

```
....
592.          snprintf(pos, sizeof(addr), "%s", ip6addr_string(ndo,
pptr));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=192
Status	New

The dangerous function, _snprintf, was found in use at line 576 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	596	596
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_ip_print(netdissect_options *ndo,

```
....
596.          snprintf(pos, sizeof(addr), "bogus address length %u",
addr_length);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=193
Status	New

The dangerous function, _snprintf, was found in use at line 625 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	642	642
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_sg_print(netdissect_options *ndo,

```
....
642.          snprintf(buf + offset, buflen - offset, ", Source %s",
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=194
Status	New

The dangerous function, _snprintf, was found in use at line 625 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	656	656
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_sg_print(netdissect_options *ndo,

```
....
656.          snprintf(buf + offset, buflen - offset, ", Group %s",
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=195
Status	New

The dangerous function, _snprintf, was found in use at line 670 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	682	682
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
682.          snprintf(pos, sizeof(rd) - (pos - rd), "%u:%u (=
%u.%u.%u.%u)",
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=196
Status	New

The dangerous function, _snprintf, was found in use at line 670 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	690	690
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
690.          snprintf(pos, sizeof(rd) - (pos - rd), "%u.%u.%u.%u:%u",
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=197
Status	New

The dangerous function, _snprintf, was found in use at line 670 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	696	696
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
696.          snprintf(pos, sizeof(rd) - (pos - rd), "%s:%u
(%u.%u.%u.%u:%u)",
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=198
Status	New

The dangerous function, _snprintf, was found in use at line 670 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	702	702
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
702.          snprintf(pos, sizeof(rd) - (pos - rd), "unknown RD
format");
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=199
Status	New

The dangerous function, _snprintf, was found in use at line 711 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	721	721
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_rt_routing_info(netdissect_options *ndo,

```
....
721.              snprintf(buf, buflen, "default route target");
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=200
Status	New

The dangerous function, _snprintf, was found in use at line 711 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	740	740
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_rt_routing_info(netdissect_options *ndo,

```
....
740.        snprintf(buf, buflen, "origin AS: %s, route target %s",
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=201
Status	New

The dangerous function, _snprintf, was found in use at line 751 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	776	776
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix4(netdissect_options *ndo,

```
....
776.        snprintf(buf, buflen, "RD: %s, %s/%d, label:%u %s",
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=202
Status	New

The dangerous function, _snprintf, was found in use at line 802 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	829	829
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_mdt_vpn_nlri(netdissect_options *ndo,

```
....
829.      snprintf(buf, buflen, "RD: %s, VPN IP Address: %s, MC Group
Address: %s",
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=203
Status	New

The dangerous function, _snprintf, was found in use at line 858 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	868	868
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
868.          snprintf(buf, buflen, "Route-Type: %s (%u), length: %u",
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=204
Status	New

The dangerous function, _snprintf, was found in use at line 858 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	877	877
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
877.              snprintf(buf + offset, buflen - offset, ", RD: %s,
Originator %s",
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=205
Status	New

The dangerous function, _snprintf, was found in use at line 858 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	885	885
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
885.              snprintf(buf + offset, buflen - offset, ", RD: %s,
Source-AS %s",
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=206
Status	New

The dangerous function, _snprintf, was found in use at line 858 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	894	894
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
894.                snprintf(buf + offset, buflen - offset, ", RD: %s",
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=207
Status	New

The dangerous function, _snprintf, was found in use at line 858 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	903	903
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
903.                snprintf(buf + offset, buflen - offset, ", Originator
%s",
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=208
Status	New

The dangerous function, _snprintf, was found in use at line 858 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	910	910
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
910.              snprintf(buf + offset, buflen - offset, ", RD: %s",
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=209
Status	New

The dangerous function, _snprintf, was found in use at line 858 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	921	921
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
921.              snprintf(buf + offset, buflen - offset, ", RD: %s,
Source-AS %s",
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=210
Status	New

The dangerous function, _snprintf, was found in use at line 965 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	982	982
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
982.            strlen=snprintf(buf, buflen, "RD: %s, BGPNH: %s",
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=211
Status	New

The dangerous function, _snprintf, was found in use at line 965 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	997	997
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
997.            strlen=snprintf(buf, buflen, "RD: %s, CE-ID: %u, Label-
Block Offset: %u, Label Base %u",
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=212
Status	New

The dangerous function, _snprintf, was found in use at line 965 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1019	1019
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
1019.                    strlen=snprintf(buf,buflen, "\n\t\tcircuit
status vector (%u) length: %u: 0x",
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=213
Status	New

The dangerous function, _snprintf, was found in use at line 965 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1028	1028
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
1028.                        strlen=snprintf(buf,buflen, "%02x",*pptr++);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=214
Status	New

The dangerous function, _snprintf, was found in use at line 965 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1036	1036
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
1036.                    strlen=snprintf(buf,buflen, "\n\t\tunknown TLV
#%u, length: %u",
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=215
Status	New

The dangerous function, _snprintf, was found in use at line 1059 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1081	1081
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix6(netdissect_options *ndo,

```
....
1081.        snprintf(buf, buflen, "%s/%d", getname6(ndo, (u_char
*)&addr), plen);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=216
Status	New

The dangerous function, _snprintf, was found in use at line 1092 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1121	1121
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_prefix6(netdissect_options *ndo,

```
....
1121.       snprintf(buf, buflen, "%s/%d, label:%u %s",
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=217
Status	New

The dangerous function, _snprintf, was found in use at line 1137 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1162	1162
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix6(netdissect_options *ndo,

```
....
1162.       snprintf(buf, buflen, "RD: %s, %s/%d, label:%u %s",
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=218
Status	New

The dangerous function, _snprintf, was found in use at line 1177 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1196	1196
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_clnp_prefix(netdissect_options *ndo,

```
....
1196.       snprintf(buf, buflen, "%s/%d",
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=219
Status	New

The dangerous function, _snprintf, was found in use at line 1207 in tcpdump/jni/tcpdump/print-bgp.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1232	1232
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_clnp_prefix(netdissect_options *ndo,

```
....
1232.       snprintf(buf, buflen, "RD: %s, %s/%d, label:%u %s",
```

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=1000001&projectid=2&pathid=17
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c

Line	262	262
Object	Namespace1434683343	Namespace1434683343

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
262.                    sizeof(ifrnetmask.ifr_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=18
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	292	292
Object	Namespace1434683343	Namespace1434683343

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
292.                        sizeof(ifrbroadaddr.ifr_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=19
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c

Line	331	331
Object	Namespace1434683343	Namespace1434683343

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
331.                        sizeof(ifrdstaddr.ifr_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=20
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-glifc.c	tcpdump/jni/libpcap/fad-glifc.c
Line	228	228
Object	Namespace734975263	Namespace734975263

Code Snippet
File Name tcpdump/jni/libpcap/fad-glifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
228.                    sizeof(ifrnetmask.lifr_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=21
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-glifc.c	tcpdump/jni/libpcap/fad-glifc.c

Line	255	255
Object	Namespace734975263	Namespace734975263

Code Snippet
File Name tcpdump/jni/libpcap/fad-glifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
255.                        sizeof(ifrbroadaddr.lifr_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=22
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-glifc.c	tcpdump/jni/libpcap/fad-glifc.c
Line	290	290
Object	Namespace734975263	Namespace734975263

Code Snippet
File Name tcpdump/jni/libpcap/fad-glifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
290.                        sizeof(ifrdstaddr.lifr_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=23
Status	New

The size of the buffer used by __pcap_nametodnaddr in unsigned, at line 491 of tcpdump/jni/libpcap/nametoaddr.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that __pcap_nametodnaddr passes to unsigned, at line 491 of tcpdump/jni/libpcap/nametoaddr.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/nametoaddr.c	tcpdump/jni/libpcap/nametoaddr.c

Line	502	502
Object	unsigned	unsigned

Code Snippet
File Name tcpdump/jni/libpcap/nametoaddr.c
Method __pcap_nametodnaddr(const char *name)

```
....
502.        memcpy((char *)&res, (char *)nep->n_addr, sizeof(unsigned
short));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=24
Status	New

The size of the buffer used by opt_blk in ->, at line 1157 of tcpdump/jni/libpcap/optimize.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that opt_blk passes to ->, at line 1157 of tcpdump/jni/libpcap/optimize.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1189	1189
Object	->	->

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_blk(struct block *b, int do_stmts)

```
....
1189.              memcpy((char *)b->val, (char *)p->pred->val, sizeof(b-
>val));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=25
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c

Line	5522	5522
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5522.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=26
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5612	5612
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5612.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=27
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c

Line	5623	5623
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5623.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=28
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5634	5634
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5634.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=29
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c

Line	5652	5652
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5652.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=30
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5693	5693
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5693.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=31
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c

Line	5705	5705
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5705.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=32
Status	New

The size of the buffer used by enter_rfmon_mode_wext in int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enter_rfmon_mode_wext passes to int, at line 5164 of tcpdump/jni/libpcap/pcap-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5730	5730
Object	int	int

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5730.            memcpy(ireq.u.name, args, sizeof (int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=33
Status	New

The size of the buffer used by pcap_read_pf in sp, at line 101 of tcpdump/jni/libpcap/pcap-pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_read_pf passes to sp, at line 101 of tcpdump/jni/libpcap/pcap-pf.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-pf.c	tcpdump/jni/libpcap/pcap-pf.c
Line	170	170

Object	sp	sp

Code Snippet
File Name tcpdump/jni/libpcap/pcap-pf.c
Method pcap_read_pf(pcap_t *pc, int cnt, pcap_handler callback, u_char *user)

```
....
170.                    memcpy((char *)sp, (char *)bp, sizeof(*sp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=34
Status	New

The size of the buffer used by read_block in bhdr, at line 256 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_block passes to bhdr, at line 256 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	315	315
Object	bhdr	bhdr

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method read_block(FILE *fp, pcap_t *p, struct block_cursor *cursor, char *errbuf)

```
....
315.        memcpy(p->buffer, &bhdr, sizeof(bhdr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=35
Status	New

The size of the buffer used by get_ai in addrinfo, at line 995 of tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_ai passes to addrinfo, at line 995 of tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Line	1008	1008

Object	addrinfo	addrinfo

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Method get_ai(pai, afd, addr)

```
....
1008.       memcpy(ai, pai, sizeof(struct addrinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=36
Status	New

The size of the buffer used by rfc1048_print in ul, at line 589 of tcpdump/jni/tcpdump/print-bootp.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rfc1048_print passes to ul, at line 589 of tcpdump/jni/tcpdump/print-bootp.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bootp.c	tcpdump/jni/tcpdump/print-bootp.c
Line	739	739
Object	ul	ul

Code Snippet
File Name tcpdump/jni/tcpdump/print-bootp.c
Method rfc1048_print(netdissect_options *ndo,

```
....
739.                            memcpy((char *)&ul, (const char *)bp,
sizeof(ul));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=37
Status	New

The size of the buffer used by rfc1048_print in ul, at line 589 of tcpdump/jni/tcpdump/print-bootp.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rfc1048_print passes to ul, at line 589 of tcpdump/jni/tcpdump/print-bootp.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bootp.c	tcpdump/jni/tcpdump/print-bootp.c
Line	742	742

Object	ul	ul

Code Snippet
File Name tcpdump/jni/tcpdump/print-bootp.c
Method rfc1048_print(netdissect_options *ndo,

```
....
742.                            memcpy((char *)&ul, (const char *)bp,
sizeof(ul));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=38
Status	New

The size of the buffer used by rfc1048_print in ul, at line 589 of tcpdump/jni/tcpdump/print-bootp.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rfc1048_print passes to ul, at line 589 of tcpdump/jni/tcpdump/print-bootp.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-bootp.c	tcpdump/jni/tcpdump/print-bootp.c
Line	968	968
Object	ul	ul

Code Snippet
File Name tcpdump/jni/tcpdump/print-bootp.c
Method rfc1048_print(netdissect_options *ndo,

```
....
968.                                memcpy((char *)&ul, (const char
*)bp, sizeof(ul));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=39
Status	New

The size of the buffer used by print_decnet_ctlmsg in srcea, at line 615 of tcpdump/jni/tcpdump/print-decnet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_decnet_ctlmsg passes to srcea, at line 615 of tcpdump/jni/tcpdump/print-decnet.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-decnet.c	tcpdump/jni/tcpdump/print-decnet.c

Line	696	696
Object	srcea	srcea

Code Snippet
File Name tcpdump/jni/tcpdump/print-decnet.c
Method print_decnet_ctlmsg(netdissect_options *ndo,

```
....
696.                sizeof(srcea));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=40
Status	New

The size of the buffer used by print_decnet_ctlmsg in srcea, at line 615 of tcpdump/jni/tcpdump/print-decnet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_decnet_ctlmsg passes to srcea, at line 615 of tcpdump/jni/tcpdump/print-decnet.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-decnet.c	tcpdump/jni/tcpdump/print-decnet.c
Line	719	719
Object	srcea	srcea

Code Snippet
File Name tcpdump/jni/tcpdump/print-decnet.c
Method print_decnet_ctlmsg(netdissect_options *ndo,

```
....
719.                sizeof(srcea));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=41
Status	New

The size of the buffer used by print_decnet_ctlmsg in rtea, at line 615 of tcpdump/jni/tcpdump/print-decnet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_decnet_ctlmsg passes to rtea, at line 615 of tcpdump/jni/tcpdump/print-decnet.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-decnet.c	tcpdump/jni/tcpdump/print-decnet.c

Line	725	725
Object	rtea	rtea

Code Snippet
File Name tcpdump/jni/tcpdump/print-decnet.c
Method print_decnet_ctlmsg(netdissect_options *ndo,

```
....
725.                sizeof(rtea));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=42
Status	New

The size of the buffer used by dnname_string in short, at line 1314 of tcpdump/jni/tcpdump/print-decnet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dnname_string passes to short, at line 1314 of tcpdump/jni/tcpdump/print-decnet.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-decnet.c	tcpdump/jni/tcpdump/print-decnet.c
Line	1321	1321
Object	short	short

Code Snippet
File Name tcpdump/jni/tcpdump/print-decnet.c
Method dnname_string(u_short dnaddr)

```
....
1321.       memcpy((char *)dna.a_addr, (char *)&dnaddr, sizeof(short));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=43
Status	New

The size of the buffer used by ns_rprint in in6_addr, at line 355 of tcpdump/jni/tcpdump/print-domain.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ns_rprint passes to in6_addr, at line 355 of tcpdump/jni/tcpdump/print-domain.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-domain.c	tcpdump/jni/tcpdump/print-domain.c

Line	492	492
Object	in6_addr	in6_addr

Code Snippet
File Name tcpdump/jni/tcpdump/print-domain.c
Method ns_rprint(netdissect_options *ndo,

```
....
492.                memcpy(&addr, cp, sizeof(struct in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=44
Status	New

The size of the buffer used by espprint_decode_encalgo in ->, at line 254 of tcpdump/jni/tcpdump/print-esp.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that espprint_decode_encalgo passes to ->, at line 254 of tcpdump/jni/tcpdump/print-esp.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	309	309
Object	->	->

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method espprint_decode_encalgo(netdissect_options *ndo,

```
....
309.                    memcpy(sa->secret, colon, sizeof(sa->secret));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=45
Status	New

The size of the buffer used by null_if_print in family, at line 75 of tcpdump/jni/tcpdump/print-null.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that null_if_print passes to family, at line 75 of tcpdump/jni/tcpdump/print-null.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-null.c	tcpdump/jni/tcpdump/print-null.c

Line	86	86
Object	family	family

Code Snippet
File Name tcpdump/jni/tcpdump/print-null.c
Method null_if_print(netdissect_options *ndo, const struct pcap_pkthdr *h, const u_char *p)

```
....
86.   memcpy((char *)&family, (char *)p, sizeof(family));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=46
Status	New

The size of the buffer used by pcap_next_etherent in e, at line 97 of tcpdump/jni/libpcap/etherent.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_next_etherent passes to e, at line 97 of tcpdump/jni/libpcap/etherent.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/etherent.c	tcpdump/jni/libpcap/etherent.c
Line	103	103
Object	e	e

Code Snippet
File Name tcpdump/jni/libpcap/etherent.c
Method pcap_next_etherent(FILE *fp)

```
....
103.        memset((char *)&e, 0, sizeof(e));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=47
Status	New

The size of the buffer used by init_val in hashtbl, at line 529 of tcpdump/jni/libpcap/optimize.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that init_val passes to hashtbl, at line 529 of tcpdump/jni/libpcap/optimize.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c

Line	534	534
Object	hashtbl	hashtbl

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method init_val(void)

```
....
534.        memset((char *)hashtbl, 0, sizeof hashtbl);
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=48
Status	New

The size of the buffer used by opt_deadstores in last, at line 1137 of tcpdump/jni/libpcap/optimize.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that opt_deadstores passes to last, at line 1137 of tcpdump/jni/libpcap/optimize.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1143	1143
Object	last	last

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_deadstores(register struct block *b)

```
....
1143.       memset((char *)last, 0, sizeof last);
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=49
Status	New

The size of the buffer used by opt_blk in ->, at line 1157 of tcpdump/jni/libpcap/optimize.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that opt_blk passes to ->, at line 1157 of tcpdump/jni/libpcap/optimize.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1181	1181

Object	->	->

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_blk(struct block *b, int do_stmts)

```
....
1181.             memset((char *)b->val, 0, sizeof(b->val));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=50
Status	New

The size of the buffer used by bt_activate in Namespace805168974, at line 183 of tcpdump/jni/libpcap/pcap-bt-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bt_activate passes to Namespace805168974, at line 183 of tcpdump/jni/libpcap/pcap-bt-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bt-linux.c	tcpdump/jni/libpcap/pcap-bt-linux.c
Line	248	248
Object	Namespace805168974	Namespace805168974

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bt-linux.c
Method bt_activate(pcap_t* handle)

```
....
248.         memset((void *) &flt.type_mask, 0xff,
sizeof(flt.type_mask));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=51
Status	New

The size of the buffer used by bt_activate in Namespace805168974, at line 183 of tcpdump/jni/libpcap/pcap-bt-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bt_activate passes to Namespace805168974, at line 183 of tcpdump/jni/libpcap/pcap-bt-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bt-linux.c	tcpdump/jni/libpcap/pcap-bt-linux.c
Line	249	249

Object	Namespace805168974	Namespace805168974

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bt-linux.c
Method bt_activate(pcap_t* handle)

```
....
249.        memset((void *) &flt.event_mask, 0xff,
sizeof(flt.event_mask));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=52
Status	New

The size of the buffer used by dlbindreq in req, at line 1309 of tcpdump/jni/libpcap/pcap-dlpi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dlbindreq passes to req, at line 1309 of tcpdump/jni/libpcap/pcap-dlpi.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	1314	1314
Object	req	req

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method dlbindreq(int fd, bpf_u_int32 sap, char *ebuf)

```
....
1314.       memset((char *)&req, 0, sizeof(req));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=53
Status	New

The size of the buffer used by get_dlpi_ppa in req, at line 1481 of tcpdump/jni/libpcap/pcap-dlpi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_dlpi_ppa passes to req, at line 1481 of tcpdump/jni/libpcap/pcap-dlpi.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	1498	1498

Object	req	req

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method get_dlpi_ppa(register int fd, register const char *device, register int unit,

```
....
1498.       memset((char *)&req, 0, sizeof(req));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=54
Status	New

The size of the buffer used by get_dlpi_ppa in buf, at line 1481 of tcpdump/jni/libpcap/pcap-dlpi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_dlpi_ppa passes to buf, at line 1481 of tcpdump/jni/libpcap/pcap-dlpi.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	1501	1501
Object	buf	buf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method get_dlpi_ppa(register int fd, register const char *device, register int unit,

```
....
1501.       memset((char *)buf, 0, sizeof(buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=55
Status	New

The size of the buffer used by esp_print_decode_onesecret in sa_list, at line 406 of tcpdump/jni/tcpdump/print-esp.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that esp_print_decode_onesecret passes to sa_list, at line 406 of tcpdump/jni/tcpdump/print-esp.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	417	417

Object	sa_list	sa_list

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
417.        memset(&sa1, 0, sizeof(struct sa_list));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=56
Status	New

The size of the buffer used by signature_verify in rcvsig, at line 119 of tcpdump/jni/tcpdump/signature.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that signature_verify passes to rcvsig, at line 119 of tcpdump/jni/tcpdump/signature.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/tcpdump/signature.c	tcpdump/jni/tcpdump/signature.c
Line	130	130
Object	rcvsig	rcvsig

Code Snippet
File Name tcpdump/jni/tcpdump/signature.c
Method signature_verify(netdissect_options *ndo,

```
....
130.      memset(sig_ptr, 0, sizeof(rcvsig));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=57
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	243	243

Object	Namespace1434683343	Namespace1434683343

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
243.                    sizeof(ifrflags.ifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=58
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	260	260
Object	Namespace1434683343	Namespace1434683343

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
260.                    sizeof(ifrnetmask.ifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=59
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	290	290

Object	Namespace1434683343	Namespace1434683343

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
290.                        sizeof(ifrbroadaddr.ifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=60
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace1434683343, at line 135 of tcpdump/jni/libpcap/fad-gifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	329	329
Object	Namespace1434683343	Namespace1434683343

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
329.                        sizeof(ifrdstaddr.ifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=61
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-glifc.c	tcpdump/jni/libpcap/fad-glifc.c
Line	209	209

Object	Namespace734975263	Namespace734975263

Code Snippet
File Name tcpdump/jni/libpcap/fad-glifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
209.                    sizeof(ifrflags.lifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=62
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-glifc.c	tcpdump/jni/libpcap/fad-glifc.c
Line	226	226
Object	Namespace734975263	Namespace734975263

Code Snippet
File Name tcpdump/jni/libpcap/fad-glifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
226.                    sizeof(ifrnetmask.lifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=63
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-glifc.c	tcpdump/jni/libpcap/fad-glifc.c
Line	253	253

Object	Namespace734975263	Namespace734975263

Code Snippet
File Name tcpdump/jni/libpcap/fad-glifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
253.                        sizeof(ifrbroadaddr.lifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=64
Status	New

The size of the buffer used by pcap_findalldevs_interfaces in Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_findalldevs_interfaces passes to Namespace734975263, at line 78 of tcpdump/jni/libpcap/fad-glifc.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/fad-glifc.c	tcpdump/jni/libpcap/fad-glifc.c
Line	288	288
Object	Namespace734975263	Namespace734975263

Code Snippet
File Name tcpdump/jni/libpcap/fad-glifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
288.                        sizeof(ifrdstaddr.lifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=65
Status	New

The size of the buffer used by pcap_can_set_rfmon_bpf in Namespace724506373, at line 633 of tcpdump/jni/libpcap/pcap-bpf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_can_set_rfmon_bpf passes to Namespace724506373, at line 633 of tcpdump/jni/libpcap/pcap-bpf.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	722	722

Object	Namespace724506373	Namespace724506373

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_can_set_rfmon_bpf(pcap_t *p)

```
....
722.         (void)strncpy(ifr.ifr_name, p->opt.source,
sizeof(ifr.ifr_name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=66
Status	New

The size of the buffer used by pcap_cleanup_bpf in Namespace724506373, at line 1271 of tcpdump/jni/libpcap/pcap-bpf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_cleanup_bpf passes to Namespace724506373, at line 1271 of tcpdump/jni/libpcap/pcap-bpf.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1304	1304
Object	Namespace724506373	Namespace724506373

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_cleanup_bpf(pcap_t *p)

```
....
1304.                                sizeof(req.ifm_name));
```

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=1000001&projectid=2&pathid=591
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/setsignal.c	tcpdump/jni/tcpdump/setsignal.c
Line	72	72
Object	neW	neW

Code Snippet
File Name tcpdump/jni/tcpdump/setsignal.c
Method struct sigaction old, new;

```
....
72.   struct sigaction old, new;
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=592
Status New

	Source	Destination
File	tcpdump/jni/libpcap/dlpisubs.c	tcpdump/jni/libpcap/dlpisubs.c
Line	229	229
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/dlpisubs.c
Method pcap_process_mactype(pcap_t *p, u_int mactype)

```
....
229.              p->dlt_list = (u_int *)malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=593
Status New

	Source	Destination
File	tcpdump/jni/libpcap/dlpisubs.c	tcpdump/jni/libpcap/dlpisubs.c
Line	329	329
Object	buffer	buffer

Code Snippet

File Name	tcpdump/jni/libpcap/dlpisubs.c
Method	pcap_alloc_databuf(pcap_t *p)

```
....
329.        p->buffer = (u_char *)malloc(p->bufsize + p->offset);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=594
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	345	345
Object	m	m

Code Snippet

File Name	tcpdump/jni/libpcap/gencode.c
Method	newchunk(n)

```
....
345.              cp->m = (void *)malloc(size);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=595
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	105	105
Object	newsa	newsa

Code Snippet

File Name	tcpdump/jni/libpcap/inet.c
Method	dup_sockaddr(struct sockaddr *sa, size_t sa_length)

```
....
105.        if ((newsa = malloc(sa_length)) == NULL)
```

Memory Leak\Path 6:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=596
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/nametoaddr.c	tcpdump/jni/libpcap/nametoaddr.c
Line	412	412
Object	ep	ep

Code Snippet
File Name tcpdump/jni/libpcap/nametoaddr.c
Method pcap_ether_aton(const char *s)

```
....
412.        e = ep = (u_char *)malloc(6);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=597
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/nametoaddr.c	tcpdump/jni/libpcap/nametoaddr.c
Line	452	452
Object	ap	ap

Code Snippet
File Name tcpdump/jni/libpcap/nametoaddr.c
Method pcap_ether_hostton(const char *name)

```
....
452.                    ap = (u_char *)malloc(6);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=598
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c

Line	1918	1918
Object	blocks	blocks

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_init(struct block *root)

```
....
1918.       blocks = (struct block **)calloc(n, sizeof(*blocks));
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=599
Status New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1926	1926
Object	edges	edges

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_init(struct block *root)

```
....
1926.       edges = (struct edge **)calloc(n_edges, sizeof(*edges));
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=600
Status New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1933	1933
Object	levels	levels

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_init(struct block *root)

```
....
1933.       levels = (struct block **)calloc(n_blocks, sizeof(*levels));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=601
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1941	1941
Object	space	space

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_init(struct block *root)

```
....
1941.       space = (bpf_u_int32 *)malloc(2 * n_blocks * nodewords *
sizeof(*space)
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=602
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1980	1980
Object	vmap	vmap

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_init(struct block *root)

```
....
1980.       vmap = (struct vmapinfo *)calloc(maxval, sizeof(*vmap));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=603
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1981	1981
Object	vnode_base	vnode_base

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method opt_init(struct block *root)

```
....
1981.        vnode_base = (struct valnode *)calloc(maxval,
sizeof(*vnode_base));
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=604
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2235	2235
Object	bf_insns	bf_insns

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method install_bpf_program(pcap_t *p, struct bpf_program *fp)

```
....
2235.        p->fcode.bf_insns = (struct bpf_insn *)malloc(prog_size);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=605
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c

Line	1661	1661
Object	wltdev	wltdev

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_activate_bpf(pcap_t *p)

```
....
1661.                          wltdev = malloc(strlen(p->opt.source) +
2);
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=606
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	2052	2052
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_activate_bpf(pcap_t *p)

```
....
2052.              p->dlt_list = (u_int *) malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=607
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	2206	2206
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_activate_bpf(pcap_t *p)

```
....
2206.       p->buffer = (u_char *)malloc(p->bufsize);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=608
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bt-linux.c	tcpdump/jni/libpcap/pcap-bt-linux.c
Line	224	224
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bt-linux.c
Method bt_activate(pcap_t* handle)

```
....
224.        handle->buffer = malloc(handle->bufsize);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=609
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bt-monitor-linux.c	tcpdump/jni/libpcap/pcap-bt-monitor-linux.c
Line	185	185
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bt-monitor-linux.c
Method bt_monitor_activate(pcap_t* handle)

```
....
185.      handle->buffer = malloc(handle->bufsize);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=610
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-can-linux.c	tcpdump/jni/libpcap/pcap-can-linux.c
Line	186	186
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-can-linux.c
Method can_activate(pcap_t* handle)

```
....
186.        handle->buffer = malloc(handle->bufsize);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=611
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	1137	1137
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_get_datalink(pcap_t *p)

```
....
1137.       if (p->dlt_list == NULL && (p->dlt_list =
malloc(255*sizeof(*(p->dlt_list)))) == NULL) {
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=612
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c

Line	189	189
Object	node	node

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method new_pcap_dag(pcap_t *p)

```
....
189.        if ((node = malloc(sizeof(pcap_dag_node_t))) == NULL) {
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=613
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-libdlpi.c	tcpdump/jni/libpcap/pcap-libdlpi.c
Line	79	79
Object	entry	entry

Code Snippet
File Name tcpdump/jni/libpcap/pcap-libdlpi.c
Method list_interfaces(const char *linkname, void *arg)

```
....
79.   if ((entry = calloc(1, sizeof(linknamelist_t))) == NULL) {
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=614
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	479	479
Object	tstamp_precision_list	tstamp_precision_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method pcap_create_interface(const char *device, char *ebuf)

```
....
479.        handle->tstamp_precision_list = malloc(2 * sizeof(u_int));
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=615
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1461	1461
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method pcap_activate_linux(pcap_t *handle)

```
....
1461.       handle->buffer     = malloc(handle->bufsize + handle->offset);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=616
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	2179	2179
Object	sys_class_net_d	sys_class_net_d

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method scan_sys_class_net(pcap_if_t **devlistp, char *errbuf)

```
....
2179.       sys_class_net_d = opendir("/sys/class/net");
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=617
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	2759	2759
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void map_arphrd_to_dlt(pcap_t *handle, int sock_fd, int arptype,

```
....
2759.                    handle->dlt_list = (u_int *)
malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=618
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	3056	3056
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void map_arphrd_to_dlt(pcap_t *handle, int sock_fd, int arptype,

```
....
3056.             handle->dlt_list = (u_int *) malloc(sizeof(u_int) *
2);
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=619
Status	New

	Source	Destination

File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	3536	3536
Object	oneshot_buffer	oneshot_buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method activate_mmap(pcap_t *handle, int *status)

```
....
3536.       handlep->oneshot_buffer = malloc(handle->snapshot);
```

Memory Leak\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=620
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	4175	4175
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method create_ring(pcap_t *handle, int *status)

```
....
4175.       handle->buffer = malloc(handle->cc * sizeof(union thdr *));
```

Memory Leak\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=621
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5830	5830
Object	tstamp_type_list	tstamp_type_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method iface_set_default_ts_types(pcap_t *handle)

```
....
5830.       handle->tstamp_type_list = malloc(NUM_SOF_TIMESTAMPING_TYPES
* sizeof(u_int));
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=622
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5897	5897
Object	tstamp_type_list	tstamp_type_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method iface_ethtool_get_ts_info(pcap_t *handle, char *ebuf)

```
....
5897.             handle->tstamp_type_list = malloc(num_ts_types *
sizeof(u_int));
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=623
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	6341	6341
Object	f	f

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method fix_program(pcap_t *handle, struct sock_fprog *fcode, int is_mmapped)

```
....
6341.       f = (struct bpf_insn *)malloc(prog_size);
```

Memory Leak\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=624
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-netfilter-linux.c	tcpdump/jni/libpcap/pcap-netfilter-linux.c
Line	500	500
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-netfilter-linux.c
Method netfilter_activate(pcap_t* handle)

```
....
500.              handle->dlt_list = (u_int *) malloc(sizeof(u_int) *
2);
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=625
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-netfilter-linux.c	tcpdump/jni/libpcap/pcap-netfilter-linux.c
Line	510	510
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-netfilter-linux.c
Method netfilter_activate(pcap_t* handle)

```
....
510.        handle->buffer = malloc(handle->bufsize);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=626
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-nit.c	tcpdump/jni/libpcap/pcap-nit.c
Line	304	304
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-nit.c
Method pcap_activate_nit(pcap_t *p)

```
....
304.        p->buffer = (u_char *)malloc(p->bufsize);
```

Memory Leak\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=627
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-nit.c	tcpdump/jni/libpcap/pcap-nit.c
Line	325	325
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-nit.c
Method pcap_activate_nit(pcap_t *p)

```
....
325.        p->dlt_list = (u_int *) malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=628
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-pf.c	tcpdump/jni/libpcap/pcap-pf.c
Line	381	381
Object	dlt_list	dlt_list

Code Snippet

File Name	tcpdump/jni/libpcap/pcap-pf.c
Method	pcap_activate_pf(pcap_t *p)

```
....
381.              p->dlt_list = (u_int *) malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=629
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-pf.c	tcpdump/jni/libpcap/pcap-pf.c
Line	479	479
Object	buffer	buffer

Code Snippet

File Name	tcpdump/jni/libpcap/pcap-pf.c
Method	pcap_activate_pf(pcap_t *p)

```
....
479.        p->buffer = (u_char*)malloc(p->bufsize + p->offset);
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=630
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-snit.c	tcpdump/jni/libpcap/pcap-snit.c
Line	381	381
Object	buffer	buffer

Code Snippet

File Name	tcpdump/jni/libpcap/pcap-snit.c
Method	pcap_activate_snit(pcap_t *p)

```
....
381.        p->buffer = (u_char *)malloc(p->bufsize);
```

Memory Leak\Path 41:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=631
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-snit.c	tcpdump/jni/libpcap/pcap-snit.c
Line	403	403
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snit.c
Method pcap_activate_snit(pcap_t *p)

```
....
403.        p->dlt_list = (u_int *) malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=632
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-snoop.c	tcpdump/jni/libpcap/pcap-snoop.c
Line	278	278
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snoop.c
Method pcap_activate_snoop(pcap_t *p)

```
....
278.            p->dlt_list = (u_int *) malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=633
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-snoop.c	tcpdump/jni/libpcap/pcap-snoop.c

Line	374	374
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snoop.c
Method pcap_activate_snoop(pcap_t *p)

```
....
374.        p->buffer = (u_char *)malloc(p->bufsize);
```

Memory Leak\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=634
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	167	167
Object	dir	dir

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_findalldevs(pcap_if_t **alldevsp, char *err_str)

```
....
167.        dir = opendir(SYS_USB_BUS_DIR);
```

Memory Leak\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=635
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	186	186
Object	dir	dir

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_findalldevs(pcap_if_t **alldevsp, char *err_str)

```
....
186.        dir = opendir(PROC_USB_BUS_DIR);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=636
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	251	251
Object	dir	dir

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method probe_devices(int bus)

```
....
251.        dir = opendir(buf);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=637
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	446	446
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_activate(pcap_t* handle)

```
....
446.        handle->buffer = malloc(handle->bufsize);
```

Memory Leak\Path 48:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=638
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-win32.c	tcpdump/jni/libpcap/pcap-win32.c
Line	559	559
Object	dlt_list	dlt_list

Code Snippet
File Name tcpdump/jni/libpcap/pcap-win32.c
Method pcap_activate_win32(pcap_t *p)

```
....
559.              p->dlt_list = (u_int *) malloc(sizeof(u_int) * 2);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=639
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-win32.c	tcpdump/jni/libpcap/pcap-win32.c
Line	666	666
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-win32.c
Method pcap_activate_win32(pcap_t *p)

```
....
666.              p->buffer = (u_char *)malloc(p->bufsize);
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=640
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	513	513

Object	tp	tp

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
513.                    tp = (u_char *)malloc(tsize);
```

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=1000001&projectid=2&pathid=715
Status	New

The variable declared in buf at tcpdump/jni/libpcap/fad-gifc.c in line 135 is not initialized when it is used by buf at tcpdump/jni/libpcap/fad-gifc.c in line 135.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	142	197
Object	buf	buf

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
142.        char *buf = NULL;
....
197.        ifrp = (struct ifreq *)buf;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=716
Status	New

The variable declared in buf at tcpdump/jni/libpcap/fad-gifc.c in line 135 is not initialized when it is used by buf at tcpdump/jni/libpcap/fad-gifc.c in line 135.

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	142	198
Object	buf	buf

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
142.        char *buf = NULL;
....
198.        ifend = (struct ifreq *)(buf + ifc.ifc_len);
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=717
Status New

The variable declared in tp at tcpdump/jni/libpcap/sf-pcap.c in line 397 is not initialized when it is used by tp at tcpdump/jni/libpcap/sf-pcap.c in line 397.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	500	521
Object	tp	tp

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
500.            static u_char *tp = NULL;
....
521.            amt_read = fread((char *)tp, 1, hdr->caplen, fp);
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=718
Status New

The variable declared in tp at tcpdump/jni/libpcap/sf-pcap.c in line 397 is not initialized when it is used by tp at tcpdump/jni/libpcap/sf-pcap.c in line 397.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	500	543
Object	tp	tp

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
500.              static u_char *tp = NULL;
....
543.              memcpy(p->buffer, (char *)tp, p->bufsize);
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=719
Status New

The variable declared in hp at tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c in line 515 is not initialized when it is used by aplist at tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c in line 515.

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Line	594	602
Object	hp	aplist

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Method explore_fqdn(pai, hostname, servname, res)

```
....
594.              hp = NULL;
....
602.        aplist = hp->h_addr_list;
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=720
Status New

The variable declared in ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1181 is not initialized when it is used by ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1181.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	1184	1189
Object	ptr	ptr

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method newhnamemem(void)

```
....
1184.       static struct hnamemem *ptr = NULL;
....
1189.               ptr = (struct hnamemem *)calloc(num, sizeof (*ptr));
```

Use of Zero Initialized Pointer\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=721
Status New

The variable declared in ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1181 is not initialized when it is used by ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1181.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	1184	1194
Object	ptr	ptr

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method newhnamemem(void)

```
....
1184.       static struct hnamemem *ptr = NULL;
....
1194.       p = ptr++;
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=722
Status New

The variable declared in ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1201 is not initialized when it is used by ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1201.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	1204	1209
Object	ptr	ptr

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method newh6namemem(void)

```
....
1204.       static struct h6namemem *ptr = NULL;
....
1209.             ptr = (struct h6namemem *)calloc(num, sizeof (*ptr));
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=723
Status New

The variable declared in ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1201 is not initialized when it is used by ptr at tcpdump/jni/tcpdump/addrtoname.c in line 1201.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	1204	1214
Object	ptr	ptr

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method newh6namemem(void)

```
....
1204.       static struct h6namemem *ptr = NULL;
....
1214.       p = ptr++;
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=724
Status New

The variable declared in rp at tcpdump/jni/tcpdump/print-domain.c in line 146 is not initialized when it is used by rp at tcpdump/jni/tcpdump/print-domain.c in line 146.

	Source	Destination
File	tcpdump/jni/tcpdump/print-domain.c	tcpdump/jni/tcpdump/print-domain.c
Line	150	163
Object	rp	rp

Code Snippet
File Name tcpdump/jni/tcpdump/print-domain.c
Method ns_nprint(netdissect_options *ndo,

```
....
150.        register const u_char *rp = NULL;
....
163.              rp = cp + l;
```

Use of Zero Initialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=725
Status New

The variable declared in rp at tcpdump/jni/tcpdump/print-domain.c in line 146 is not initialized when it is used by rp at tcpdump/jni/tcpdump/print-domain.c in line 146.

	Source	Destination
File	tcpdump/jni/tcpdump/print-domain.c	tcpdump/jni/tcpdump/print-domain.c
Line	150	170
Object	rp	rp

Code Snippet
File Name tcpdump/jni/tcpdump/print-domain.c
Method ns_nprint(netdissect_options *ndo,

```
....
150.        register const u_char *rp = NULL;
....
170.                                  rp = cp + 1;
```

Use of Zero Initialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=726
Status New

The variable declared in rp at tcpdump/jni/tcpdump/print-domain.c in line 146 is not initialized when it is used by rp at tcpdump/jni/tcpdump/print-domain.c in line 146.

	Source	Destination
File	tcpdump/jni/tcpdump/print-domain.c	tcpdump/jni/tcpdump/print-domain.c
Line	150	222
Object	rp	rp

Code Snippet
File Name tcpdump/jni/tcpdump/print-domain.c
Method ns_nprint(netdissect_options *ndo,

```
....
150.        register const u_char *rp = NULL;
....
222.                            rp += l + 1;
```

Use of Zero Initialized Pointer\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=727
Status New

The variable declared in root at tcpdump/jni/libpcap/gencode.c in line 430 is not initialized when it is used by bf_insns at tcpdump/jni/libpcap/gencode.c in line 430.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	465	508
Object	root	bf_insns

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method pcap_compile(pcap_t *p, struct bpf_program *program,

```
....
465.        root = NULL;
....
508.        program->bf_insns = icode_to_fcode(root, &len);
```

Use of Zero Initialized Pointer\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=728
Status New

The variable declared in BinaryExpr at tcpdump/jni/libpcap/optimize.c in line 2005 is not initialized when it is used by bf_insns at tcpdump/jni/libpcap/optimize.c in line 2247.

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2012	2261
Object	BinaryExpr	bf_insns

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method convert_code_r(struct block *p)

```
....
2012.       struct slist **offset = NULL;
```

File Name tcpdump/jni/libpcap/optimize.c
Method dot_dump_node(struct block *block, struct bpf_program *prog, FILE *out)

```
....
2261.             fprintf(out, "\\n%s", bpf_image(prog->bf_insns + i,
i));
```

Use of Zero Initialized Pointer\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=729
Status New

The variable declared in BinaryExpr at tcpdump/jni/libpcap/optimize.c in line 2005 is not initialized when it is used by bf_insns at tcpdump/jni/libpcap/optimize.c in line 2313.

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2012	2319
Object	BinaryExpr	bf_insns

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method convert_code_r(struct block *p)

```
....
2012.       struct slist **offset = NULL;
```

File Name	tcpdump/jni/libpcap/optimize.c
Method	dot_dump(struct block *root)

```
....
2319.       f.bf_insns = icode_to_fcode(root, &f.bf_len);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=730
Status	New

The variable declared in BinaryExpr at tcpdump/jni/libpcap/optimize.c in line 2005 is not initialized when it is used by bf_insns at tcpdump/jni/libpcap/optimize.c in line 2332.

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2012	2337
Object	BinaryExpr	bf_insns

Code Snippet

File Name	tcpdump/jni/libpcap/optimize.c
Method	convert_code_r(struct block *p)

```
....
2012.       struct slist **offset = NULL;
```

File Name	tcpdump/jni/libpcap/optimize.c
Method	plain_dump(struct block *root)

```
....
2337.       f.bf_insns = icode_to_fcode(root, &f.bf_len);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=731
Status	New

The variable declared in description at tcpdump/jni/libpcap/inet.c in line 492 is not initialized when it is used by description at tcpdump/jni/libpcap/inet.c in line 181.

	Source	Destination

File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	561	338
Object	description	description

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method get_if_description(const char *name)

```
....
561.                    description = NULL;
```

File Name tcpdump/jni/libpcap/inet.c
Method add_or_find_if(pcap_if_t **curdev_ret, pcap_if_t **alldevs, const char *name,

```
....
338.                    curdev->description = strdup(description);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=732
Status	New

The variable declared in description at tcpdump/jni/libpcap/inet.c in line 492 is not initialized when it is used by description at tcpdump/jni/libpcap/inet.c in line 181.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	495	338
Object	description	description

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method get_if_description(const char *name)

```
....
495.        char *description = NULL;
```

File Name tcpdump/jni/libpcap/inet.c
Method add_or_find_if(pcap_if_t **curdev_ret, pcap_if_t **alldevs, const char *name,

```
....
338.                    curdev->description = strdup(description);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=733
Status	New

The variable declared in netmask at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by addresses at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	694	745
Object	netmask	addresses

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
694.                curaddr->netmask = NULL;
....
745.                curdev->addresses = curaddr;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=734
Status	New

The variable declared in broadaddr at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by addresses at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	709	745
Object	broadaddr	addresses

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
709.                curaddr->broadaddr = NULL;
....
745.                curdev->addresses = curaddr;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=735
Status	New

The variable declared in dstaddr at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by addresses at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	726	745
Object	dstaddr	addresses

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
726.              curaddr->dstaddr = NULL;
....
745.              curdev->addresses = curaddr;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=736
Status	New

The variable declared in addr at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by addresses at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	681	745
Object	addr	addresses

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
681.              curaddr->addr = NULL;
....
745.              curdev->addresses = curaddr;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=737
Status	New

The variable declared in next at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by addresses at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	671	745
Object	next	addresses

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
671.         curaddr->next = NULL;
....
745.               curdev->addresses = curaddr;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=738
Status	New

The variable declared in next at tcpdump/jni/libpcap/pcap-snf.c in line 325 is not initialized when it is used by addresses at tcpdump/jni/libpcap/pcap-snf.c in line 325.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-snf.c	tcpdump/jni/libpcap/pcap-snf.c
Line	392	391
Object	next	addresses

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snf.c
Method snf_findalldevs(pcap_if_t **devlistp, char *errbuf)

```
....
392.               curaddr->next = NULL;
....
391.               curdev->addresses = curaddr;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=739
Status	New

The variable declared in next at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by next at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	671	751
Object	next	next

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
671.         curaddr->next = NULL;
....
751.                 prevaddr->next = curaddr;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=740
Status	New

The variable declared in addr at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by next at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	681	751
Object	addr	next

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
681.                 curaddr->addr = NULL;
....
751.                 prevaddr->next = curaddr;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=741
Status	New

The variable declared in netmask at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by next at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	694	751
Object	netmask	next

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
694.                curaddr->netmask = NULL;
....
751.                prevaddr->next = curaddr;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=742
Status	New

The variable declared in dstaddr at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by next at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	726	751
Object	dstaddr	next

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
726.                curaddr->dstaddr = NULL;
....
751.                prevaddr->next = curaddr;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=743
Status	New

The variable declared in broadaddr at tcpdump/jni/libpcap/inet.c in line 655 is not initialized when it is used by next at tcpdump/jni/libpcap/inet.c in line 655.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	709	751
Object	broadaddr	next

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_addr_to_dev(pcap_if_t *curdev,

```
....
709.                curaddr->broadaddr = NULL;
....
751.                prevaddr->next = curaddr;
```

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=1000001&projectid=2&pathid=127
Status	New

Calling free() (line 6094) on a variable that was not dynamically allocated (line 6094) in file tcpdump/jni/libpcap/gencode.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	6146	6146
Object	eaddr	eaddr

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method gen_scode(name, q)

```
....
6146.                           free(eaddr);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=128
Status	New

Calling free() (line 6094) on a variable that was not dynamically allocated (line 6094) in file tcpdump/jni/libpcap/gencode.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	6155	6155
Object	eaddr	eaddr

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method gen_scode(name, q)

```
....
6155.                           free(eaddr);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=129
Status	New

Calling free() (line 6094) on a variable that was not dynamically allocated (line 6094) in file tcpdump/jni/libpcap/gencode.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	6164	6164
Object	eaddr	eaddr

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method gen_scode(name, q)

```
....
6164.                           free(eaddr);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=130
Status	New

Calling free() (line 6094) on a variable that was not dynamically allocated (line 6094) in file tcpdump/jni/libpcap/gencode.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	6177	6177
Object	eaddr	eaddr

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method gen_scode(name, q)

```
....
6177.                           free(eaddr);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=131
Status	New

Calling free() (line 6094) on a variable that was not dynamically allocated (line 6094) in file tcpdump/jni/libpcap/gencode.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	6186	6186
Object	eaddr	eaddr

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method gen_scode(name, q)

```
....
6186.                          free(eaddr);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=132
Status	New

Calling free() (line 6094) on a variable that was not dynamically allocated (line 6094) in file tcpdump/jni/libpcap/gencode.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	6366	6366
Object	eaddr	eaddr

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method gen_scode(name, q)

```
....
6366.              free(eaddr);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=133
Status	New

Calling free() (line 789) on a variable that was not dynamically allocated (line 789) in file tcpdump/jni/libpcap/inet.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	810	810
Object	curaddr	curaddr

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method pcap_freealldevs(pcap_if_t *alldevs)

```
....
810.                    free(curaddr);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=134
Status	New

Calling free() (line 789) on a variable that was not dynamically allocated (line 789) in file tcpdump/jni/libpcap/inet.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	827	827
Object	curdev	curdev

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method pcap_freealldevs(pcap_if_t *alldevs)

```
....
827.                free(curdev);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=135
Status	New

Calling free() (line 274) on a variable that was not dynamically allocated (line 274) in file tcpdump/jni/libpcap/pcap-libdlpi.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-libdlpi.c	tcpdump/jni/libpcap/pcap-libdlpi.c
Line	302	302
Object	entry	entry

Code Snippet
File Name tcpdump/jni/libpcap/pcap-libdlpi.c
Method pcap_platform_finddevs(pcap_if_t **alldevsp, char *errbuf)

```
....
302.                free(entry);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=136
Status	New

Calling free() (line 545) on a variable that was not dynamically allocated (line 545) in file tcpdump/jni/libpcap/pcap-linux.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	567	567
Object	pathstr	pathstr

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method get_mac80211_phydev(pcap_t *handle, const char *device, char *phydev_path,

```
....
567.                    free(pathstr);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=137
Status	New

Calling free() (line 545) on a variable that was not dynamically allocated (line 545) in file tcpdump/jni/libpcap/pcap-linux.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	573	573
Object	pathstr	pathstr

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method get_mac80211_phydev(pcap_t *handle, const char *device, char *phydev_path,

```
....
573.                free(pathstr);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=138
Status	New

Calling free() (line 545) on a variable that was not dynamically allocated (line 545) in file tcpdump/jni/libpcap/pcap-linux.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	576	576
Object	pathstr	pathstr

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method get_mac80211_phydev(pcap_t *handle, const char *device, char *phydev_path,

```
....
576.        free(pathstr);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=139
Status	New

Calling free() (line 515) on a variable that was not dynamically allocated (line 515) in file tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Line	675	675
Object	aplist	aplist

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Method explore_fqdn(pai, hostname, servname, res)

```
....
675.                free(aplist);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=140
Status	New

Calling free() (line 515) on a variable that was not dynamically allocated (line 515) in file tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Line	677	677
Object	apbuf	apbuf

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Method explore_fqdn(pai, hostname, servname, res)

```
....
677.                free(apbuf);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=141
Status	New

Calling free() (line 912) on a variable that was not dynamically allocated (line 912) in file tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Line	969	969
Object	ap	ap

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Method get_name(addr, afd, res, numaddr, pai, servname)

```
....
969.            free(ap);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=142
Status	New

Calling free() (line 912) on a variable that was not dynamically allocated (line 912) in file tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c may result with a crash.

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c	tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Line	971	971
Object	cn	cn

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getaddrinfo.c
Method get_name(addr, afd, res, numaddr, pai, servname)

```
....
971.            free(cn);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=143
Status	New

Calling free() (line 999) on a variable that was not dynamically allocated (line 999) in file tcpdump/jni/tcpdump/tcpdump.c may result with a crash.

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	1783	1783
Object	cmdbuf	cmdbuf

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method main(int argc, char **argv)

```
....
1783.               free(cmdbuf);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=144
Status	New

Calling free() (line 999) on a variable that was not dynamically allocated (line 999) in file tcpdump/jni/tcpdump/tcpdump.c may result with a crash.

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	2078	2078
Object	cmdbuf	cmdbuf

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method main(int argc, char **argv)

```
....
2078.       free(cmdbuf);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=145
Status	New

Calling free() (line 145) on a variable that was not dynamically allocated (line 145) in file tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c may result with a crash.

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	152	152
Object	e	e

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method static void free_ethers (void)

```
....
152.        free(e);
```

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=1000001&projectid=2&pathid=146
Status	New

The function NameLength in tcpdump/jni/libpcap/fad-win32.c at line 122 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	tcpdump/jni/libpcap/fad-win32.c	tcpdump/jni/libpcap/fad-win32.c
Line	163	163
Object	NameLength	NameLength

Code Snippet
File Name tcpdump/jni/libpcap/fad-win32.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
163.                AdaptersName = (char*) malloc(NameLength);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=147
Status	New

The function size in tcpdump/jni/libpcap/gencode.c at line 324 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	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	345	345
Object	size	size

Code Snippet	
File Name	tcpdump/jni/libpcap/gencode.c
Method	newchunk(n)

```
....
345.              cp->m = (void *)malloc(size);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=148
Status	New

The function descrlen in tcpdump/jni/libpcap/inet.c at line 492 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	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	520	520
Object	descrlen	descrlen

Code Snippet	
File Name	tcpdump/jni/libpcap/inet.c
Method	get_if_description(const char *name)

```
....
520.                    if ((description = malloc(descrlen)) != NULL) {
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=149
Status	New

The function sz in tcpdump/jni/libpcap/missing/snprintf.c at line 459 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	tcpdump/jni/libpcap/missing/snprintf.c	tcpdump/jni/libpcap/missing/snprintf.c
Line	472	472
Object	sz	sz

Code Snippet

File Name	tcpdump/jni/libpcap/missing/snprintf.c
Method	snprintf (char *str, size_t sz, const char *format, ...)

```
....
472.      tmp = malloc (sz);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=150
Status	New

The function prog_size in tcpdump/jni/libpcap/optimize.c at line 2215 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	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2235	2235
Object	prog_size	prog_size

Code Snippet	
File Name	tcpdump/jni/libpcap/optimize.c
Method	install_bpf_program(pcap_t *p, struct bpf_program *fp)

```
....
2235.       p->fcode.bf_insns = (struct bpf_insn *)malloc(prog_size);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=151
Status	New

The function prog_size in tcpdump/jni/libpcap/pcap-linux.c at line 6326 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	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	6341	6341
Object	prog_size	prog_size

Code Snippet	
File Name	tcpdump/jni/libpcap/pcap-linux.c

Method	fix_program(pcap_t *handle, struct sock_fprog *fcode, int is_mmapped)

```
....
6341.       f = (struct bpf_insn *)malloc(prog_size);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=152
Status	New

The function tsize in tcpdump/jni/libpcap/sf-pcap.c at line 397 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	513	513
Object	tsize	tsize

Code Snippet	
File Name	tcpdump/jni/libpcap/sf-pcap.c
Method	pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
513.                   tp = (u_char *)malloc(tsize);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=153
Status	New

The function sz in tcpdump/jni/tcpdump/missing/snprintf.c at line 459 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	tcpdump/jni/tcpdump/missing/snprintf.c	tcpdump/jni/tcpdump/missing/snprintf.c
Line	472	472
Object	sz	sz

Code Snippet	
File Name	tcpdump/jni/tcpdump/missing/snprintf.c
Method	snprintf (char *str, size_t sz, const char *format, ...)

```
....
472.      tmp = malloc (sz);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=154
Status	New

The function len in tcpdump/jni/tcpdump/missing/strdup.c at line 41 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	tcpdump/jni/tcpdump/missing/strdup.c	tcpdump/jni/tcpdump/missing/strdup.c
Line	48	48
Object	len	len

Code Snippet
File Name tcpdump/jni/tcpdump/missing/strdup.c
Method strdup(str)

```
....
48.   if ((copy = malloc(len)) == NULL)
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=155
Status	New

The function en_name_len in tcpdump/jni/libpcap/inet.c at line 181 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	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	240	240
Object	en_name_len	en_name_len

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_or_find_if(pcap_if_t **curdev_ret, pcap_if_t **alldevs, const char *name,

```
....
240.                    en_name = malloc(en_name_len + 1);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=156
Status	New

The function length in tcpdump/jni/libpcap/pcap-win32.c at line 781 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	tcpdump/jni/libpcap/pcap-win32.c	tcpdump/jni/libpcap/pcap-win32.c
Line	800	800
Object	length	length

Code Snippet
File Name tcpdump/jni/libpcap/pcap-win32.c
Method pcap_create_interface(const char *device, char *ebuf)

```
....
800.              deviceAscii = (char*)malloc(length + 1);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=157
Status	New

The function siz in tcpdump/jni/tcpdump/print-decnet.c at line 1299 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	tcpdump/jni/tcpdump/print-decnet.c	tcpdump/jni/tcpdump/print-decnet.c
Line	1306	1306
Object	siz	siz

Code Snippet
File Name tcpdump/jni/tcpdump/print-decnet.c
Method dnnum_string(u_short dnaddr)

```
....
1306.       str = (char *)malloc(siz = sizeof("00.0000"));
```

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=1000001&projectid=2&pathid=159
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 377 of tcpdump/jni/tcpdump/print-ntp.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/print-ntp.c	tcpdump/jni/tcpdump/print-ntp.c
Line	424	424
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-ntp.c
Method p_ntp_delta(netdissect_options *ndo,

```
....
424.        f = ff * 1000000000.0;  /* treat fraction as parts per
billion */
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=160
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 325 of tcpdump/jni/tcpdump/print-ntp.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	tcpdump/jni/tcpdump/print-ntp.c	tcpdump/jni/tcpdump/print-ntp.c
Line	335	335
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-ntp.c
Method p_sfix(netdissect_options *ndo,

```
....
335.        f = ff * 1000000.0;     /* Treat fraction as parts per
million */
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=161
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 342 of tcpdump/jni/tcpdump/print-ntp.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/print-ntp.c	tcpdump/jni/tcpdump/print-ntp.c
Line	356	356
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-ntp.c
Method p_ntp_time(netdissect_options *ndo,

```
....
356.        f = ff * 1000000000.0;  /* treat fraction as parts per
billion */
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=162
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 314 of tcpdump/jni/libpcap/pcap-libdlpi.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	tcpdump/jni/libpcap/pcap-libdlpi.c	tcpdump/jni/libpcap/pcap-libdlpi.c
Line	358	358
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/libpcap/pcap-libdlpi.c
Method pcap_read_libdlpi(pcap_t *p, int count, pcap_handler callback, u_char *user)

```
....
358.                len = msglen;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=163
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4473 of tcpdump/jni/libpcap/scanner.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4502	4502
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static void pcap_ensure_buffer_stack (void)

```
....
4502.                num_to_alloc = (yy_buffer_stack_max) + grow_size;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=164
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3986 of tcpdump/jni/libpcap/scanner.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c

Line	4076	4076
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static int yy_get_next_buffer (void)

```
....
4076.             YY_INPUT( (&YY_CURRENT_BUFFER_LVALUE-
>yy_ch_buf[number_to_move]),
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=165
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 276 of tcpdump/jni/tcpdump/print-dhcp6.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/print-dhcp6.c	tcpdump/jni/tcpdump/print-dhcp6.c
Line	724	724
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-dhcp6.c
Method dhcp6opt_print(netdissect_options *ndo,

```
....
724.                    remain_len = optlen;
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=746
Status	New

The size of the buffer used by process_idb_options in tsresol_opt, at line 403 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_bytes passes to buf, at line 231 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	462
Object	buf	tsresol_opt

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.        amt_read = fread(buf, 1, bytes_to_read, fp);
```

File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method process_idb_options(pcap_t *p, struct block_cursor *cursor, u_int *tsresol,

```
....
462.                    memcpy(&tsresol_opt, optvalue,
sizeof(tsresol_opt));
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=747
Status	New

The size of the buffer used by process_idb_options in Pointer, at line 403 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_bytes passes to buf, at line 231 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	506
Object	buf	Pointer

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.        amt_read = fread(buf, 1, bytes_to_read, fp);
```

File Name tcpdump/jni/libpcap/sf-pcap-ng.c

Method process_idb_options(pcap_t *p, struct block_cursor *cursor, u_int *tsresol,

```
....
506.                    memcpy(tsoffset, optvalue, sizeof(*tsoffset));
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=748
Status	New

The size of the buffer used by process_idb_options in tsoffset, at line 403 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_bytes passes to buf, at line 231 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	506
Object	buf	tsoffset

Code Snippet

File Name tcpdump/jni/libpcap/sf-pcap-ng.c

Method read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.        amt_read = fread(buf, 1, bytes_to_read, fp);
```

File Name tcpdump/jni/libpcap/sf-pcap-ng.c

Method process_idb_options(pcap_t *p, struct block_cursor *cursor, u_int *tsresol,

```
....
506.                    memcpy(tsoffset, optvalue, sizeof(*tsoffset));
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=749
Status	New

The size of the buffer used by process_idb_options in sizeof, at line 403 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_bytes passes to buf, at line 231 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	462
Object	buf	sizeof

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.         amt_read = fread(buf, 1, bytes_to_read, fp);
```

File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method process_idb_options(pcap_t *p, struct block_cursor *cursor, u_int *tsresol,

```
....
462.                     memcpy(&tsresol_opt, optvalue,
sizeof(tsresol_opt));
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=750
Status	New

The size of the buffer used by process_idb_options in sizeof, at line 403 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_bytes passes to buf, at line 231 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	506
Object	buf	sizeof

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.        amt_read = fread(buf, 1, bytes_to_read, fp);
```

File Name tcpdump/jni/libpcap/sf-pcap-ng.c

Method process_idb_options(pcap_t *p, struct block_cursor *cursor, u_int *tsresol,

```
....
506.                    memcpy(tsoffset, optvalue, sizeof(*tsoffset));
```

Stored Buffer Overflow boundcpy\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=751
Status	New

The size of the buffer used by read_block in sizeof, at line 256 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_bytes passes to buf, at line 231 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	315
Object	buf	sizeof

Code Snippet

File Name tcpdump/jni/libpcap/sf-pcap-ng.c

Method read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.        amt_read = fread(buf, 1, bytes_to_read, fp);
```

File Name tcpdump/jni/libpcap/sf-pcap-ng.c

Method read_block(FILE *fp, pcap_t *p, struct block_cursor *cursor, char *errbuf)

```
....
315.        memcpy(p->buffer, &bhdr, sizeof(bhdr));
```

Stored Buffer Overflow boundcpy\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=752
Status	New

The size of the buffer used by read_block in bhdr, at line 256 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_bytes passes to buf, at line 231 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	315
Object	buf	bhdr

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.        amt_read = fread(buf, 1, bytes_to_read, fp);
```

File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method read_block(FILE *fp, pcap_t *p, struct block_cursor *cursor, char *errbuf)

```
....
315.        memcpy(p->buffer, &bhdr, sizeof(bhdr));
```

Inadequate Encryption Strength

Query Path:
CPP\Cx\CPP Medium Threat\Inadequate Encryption Strength Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-13 Cryptographic Protection (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description
Inadequate Encryption Strength\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=690
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 803 of tcpdump/jni/tcpdump/print-tcp.c, to protect sensitive personal information ndo_sigsecret, from tcpdump/jni/tcpdump/print-tcp.c at line 803.

	Source	Destination
File	tcpdump/jni/tcpdump/print-tcp.c	tcpdump/jni/tcpdump/print-tcp.c
Line	881	881
Object	ndo_sigsecret	MD5_Update

Code Snippet
File Name tcpdump/jni/tcpdump/print-tcp.c
Method tcp_verify_signature(netdissect_options *ndo,

```
....
881.          MD5_Update(&ctx, ndo->ndo_sigsecret, strlen(ndo-
>ndo_sigsecret));
```

Inadequate Encryption Strength\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=691
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 803 of tcpdump/jni/tcpdump/print-tcp.c, to protect sensitive personal information ndo_sigsecret, from tcpdump/jni/tcpdump/print-tcp.c at line 803.

	Source	Destination
File	tcpdump/jni/tcpdump/print-tcp.c	tcpdump/jni/tcpdump/print-tcp.c
Line	881	881
Object	ndo_sigsecret	MD5_Update

Code Snippet
File Name tcpdump/jni/tcpdump/print-tcp.c
Method tcp_verify_signature(netdissect_options *ndo,

```
....
881.          MD5_Update(&ctx, ndo->ndo_sigsecret, strlen(ndo-
>ndo_sigsecret));
```

Inadequate Encryption Strength\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=692
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 49 of tcpdump/jni/tcpdump/signature.c, to protect sensitive personal information ndo_sigsecret, from tcpdump/jni/tcpdump/signature.c at line 119.

	Source	Destination
File	tcpdump/jni/tcpdump/signature.c	tcpdump/jni/tcpdump/signature.c
Line	137	64
Object	ndo_sigsecret	MD5_Update

Code Snippet
File Name tcpdump/jni/tcpdump/signature.c
Method signature_verify(netdissect_options *ndo,

```
....
137.                                    strlen(ndo->ndo_sigsecret), sig);
```

File Name tcpdump/jni/tcpdump/signature.c

Method signature_compute_hmac_md5(const uint8_t *text, int text_len, unsigned char *key,

```
....
64.           MD5_Update(&tctx, key, key_len);
```

Inadequate Encryption Strength\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=693
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 49 of tcpdump/jni/tcpdump/signature.c, to protect sensitive personal information ndo_sigsecret, from tcpdump/jni/tcpdump/signature.c at line 119.

	Source	Destination
File	tcpdump/jni/tcpdump/signature.c	tcpdump/jni/tcpdump/signature.c
Line	136	64
Object	ndo_sigsecret	MD5_Update

Code Snippet
File Name tcpdump/jni/tcpdump/signature.c
Method signature_verify(netdissect_options *ndo,

```
....
136.      signature_compute_hmac_md5(pptr, plen, (unsigned char *)ndo-
>ndo_sigsecret,
```

File Name tcpdump/jni/tcpdump/signature.c

Method signature_compute_hmac_md5(const uint8_t *text, int text_len, unsigned char *key,

```
....
64.           MD5_Update(&tctx, key, key_len);
```

Inadequate Encryption Strength\Path 5:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=694
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 49 of tcpdump/jni/tcpdump/signature.c, to protect sensitive personal information ndo_sigsecret, from tcpdump/jni/tcpdump/signature.c at line 119.

	Source	Destination
File	tcpdump/jni/tcpdump/signature.c	tcpdump/jni/tcpdump/signature.c
Line	136	98
Object	ndo_sigsecret	MD5_Update

Code Snippet

File Name tcpdump/jni/tcpdump/signature.c

Method signature_verify(netdissect_options *ndo,

```
....
136.      signature_compute_hmac_md5(pptr, plen, (unsigned char *)ndo-
>ndo_sigsecret,
```

File Name tcpdump/jni/tcpdump/signature.c

Method signature_compute_hmac_md5(const uint8_t *text, int text_len, unsigned char *key,

```
....
98.      MD5_Update(&context, k_ipad, 64);     /* start with inner pad
*/
```

Inadequate Encryption Strength\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=695
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 49 of tcpdump/jni/tcpdump/signature.c, to protect sensitive personal information ndo_sigsecret, from tcpdump/jni/tcpdump/signature.c at line 119.

	Source	Destination
File	tcpdump/jni/tcpdump/signature.c	tcpdump/jni/tcpdump/signature.c
Line	136	106
Object	ndo_sigsecret	MD5_Update

Code Snippet

File Name tcpdump/jni/tcpdump/signature.c

Method	signature_verify(netdissect_options *ndo,

```
....
136.      signature_compute_hmac_md5(pptr, plen, (unsigned char *)ndo-
>ndo_sigsecret,
```

File Name	tcpdump/jni/tcpdump/signature.c
Method	signature_compute_hmac_md5(const uint8_t *text, int text_len, unsigned char *key,

```
....
106.      MD5_Update(&context, k_opad, 64);     /* start with outer pad
*/
```

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=1000001&projectid=2&pathid=13
Status	New

The pointer us1 at tcpdump/jni/tcpdump/strcasecmp.c in line 62 is being used after it has been freed.

	Source	Destination
File	tcpdump/jni/tcpdump/strcasecmp.c	tcpdump/jni/tcpdump/strcasecmp.c
Line	72	72
Object	us1	us1

Code Snippet

File Name	tcpdump/jni/tcpdump/strcasecmp.c
Method	strcasecmp(s1, s2)

```
....
72.   return(cm[*us1] - cm[*--us2]);
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=14
Status	New

The pointer us1 at tcpdump/jni/tcpdump/strcasecmp.c in line 76 is being used after it has been freed.

	Source	Destination
File	tcpdump/jni/tcpdump/strcasecmp.c	tcpdump/jni/tcpdump/strcasecmp.c
Line	87	87
Object	us1	us1

Code Snippet
File Name tcpdump/jni/tcpdump/strcasecmp.c
Method strncasecmp(s1, s2, n)

```
....
87.    return(n < 0 ? 0 : cm[*us1] - cm[*--us2]);
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=15
Status	New

The pointer us2 at tcpdump/jni/tcpdump/strcasecmp.c in line 62 is being used after it has been freed.

	Source	Destination
File	tcpdump/jni/tcpdump/strcasecmp.c	tcpdump/jni/tcpdump/strcasecmp.c
Line	72	72
Object	us2	us2

Code Snippet
File Name tcpdump/jni/tcpdump/strcasecmp.c
Method strcasecmp(s1, s2)

```
....
72.    return(cm[*us1] - cm[*--us2]);
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=16
Status	New

The pointer us2 at tcpdump/jni/tcpdump/strcasecmp.c in line 76 is being used after it has been freed.

	Source	Destination
File	tcpdump/jni/tcpdump/strcasecmp.c	tcpdump/jni/tcpdump/strcasecmp.c
Line	87	87
Object	us2	us2

Code Snippet
File Name tcpdump/jni/tcpdump/strcasecmp.c
Method strncasecmp(s1, s2, n)

```
....
87.   return(n < 0 ? 0 : cm[*us1] - cm[*--us2]);
```

Short Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Short Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description
Short Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=166
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 245 of tcpdump/jni/libpcap/pcap-dag.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	408	408
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_read(pcap_t *p, int cnt, pcap_handler callback, u_char *user)

```
....
408.                     packet_len += (8 * num_ext_hdr);
```

Short Overflow\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=167
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 140 of tcpdump/jni/tcpdump/checksum.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/checksum.c	tcpdump/jni/tcpdump/checksum.c
Line	187	187
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/checksum.c
Method create_osi_cksum (const uint8_t *pptr, int checksum_offset, int length)

```
....
187.      checksum = ((x << 8) | y);
```

Short Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=168
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 364 of tcpdump/jni/tcpdump/print-atm.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atm.c	tcpdump/jni/tcpdump/print-atm.c
Line	381	381
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-atm.c
Method oam_print (netdissect_options *ndo,

```
....
381.      vpi = (cell_header>>20)&0xff;
```

Short Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=169
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 364 of tcpdump/jni/tcpdump/print-atm.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atm.c	tcpdump/jni/tcpdump/print-atm.c
Line	382	382
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-atm.c
Method oam_print (netdissect_options *ndo,

```
....
382.      vci = (cell_header>>4)&0xffff;
```

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=1000001&projectid=2&pathid=123
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 364 of tcpdump/jni/tcpdump/print-atm.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atm.c	tcpdump/jni/tcpdump/print-atm.c
Line	383	383
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-atm.c
Method oam_print (netdissect_options *ndo,

```
....
383.      payload = (cell_header>>1)&0x7;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=124
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 364 of tcpdump/jni/tcpdump/print-atm.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tcpdump/jni/tcpdump/print-atm.c	tcpdump/jni/tcpdump/print-atm.c
Line	384	384
Object	AssignExpr	AssignExpr

Code Snippet
File Name tcpdump/jni/tcpdump/print-atm.c
Method oam_print (netdissect_options *ndo,

```
....
384.      clp = cell_header&0x1;
```

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=1000001&projectid=2&pathid=125
Status	New

The application performs an illegal operation in bpf_filter_with_aux_data, in tcpdump/jni/libpcap/bpf/net/bpf_filter.c. In line 221, the program attempts to divide by X, 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 X in bpf_filter_with_aux_data of tcpdump/jni/libpcap/bpf/net/bpf_filter.c, at line 221.

	Source	Destination
File	tcpdump/jni/libpcap/bpf/net/bpf_filter.c	tcpdump/jni/libpcap/bpf/net/bpf_filter.c
Line	510	510
Object	X	X

Code Snippet
File Name tcpdump/jni/libpcap/bpf/net/bpf_filter.c
Method bpf_filter_with_aux_data(pc, p, wirelen, buflen, aux_data)

```
....
510.                    A /= X;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=126
Status	New

The application performs an illegal operation in bpf_filter_with_aux_data, in tcpdump/jni/libpcap/bpf/net/bpf_filter.c. In line 221, the program attempts to divide by X, 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 X in bpf_filter_with_aux_data of tcpdump/jni/libpcap/bpf/net/bpf_filter.c, at line 221.

	Source	Destination
File	tcpdump/jni/libpcap/bpf/net/bpf_filter.c	tcpdump/jni/libpcap/bpf/net/bpf_filter.c
Line	516	516
Object	X	X

Code Snippet
File Name tcpdump/jni/libpcap/bpf/net/bpf_filter.c
Method bpf_filter_with_aux_data(pc, p, wirelen, buflen, aux_data)

```
....
516.                    A %= X;
```

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=1000001&projectid=2&pathid=589
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/fad-gifc.c	tcpdump/jni/libpcap/fad-gifc.c
Line	193	402
Object	buf	buf

Code Snippet
File Name tcpdump/jni/libpcap/fad-gifc.c
Method pcap_findalldevs_interfaces(pcap_if_t **alldevsp, char *errbuf)

```
....
193.                free(buf);
....
402.        free(buf);
```

Double Free\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=590
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	1783	2078
Object	cmdbuf	cmdbuf

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method main(int argc, char **argv)

```
....
1783.                free(cmdbuf);
....
2078.        free(cmdbuf);
```

Wrong Memory Allocation

Query Path:
CPP\Cx\CPP Medium Threat\Wrong Memory Allocation Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Wrong Memory Allocation\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=744
Status New

The function malloc in tcpdump/jni/libpcap/pcap-snf.c at line 325 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	tcpdump/jni/libpcap/pcap-snf.c	tcpdump/jni/libpcap/pcap-snf.c
Line	393	393
Object	sizeof	malloc

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snf.c
Method snf_findalldevs(pcap_if_t **devlistp, char *errbuf)

```
....
393.              curaddr->addr = (struct sockaddr*)malloc(sizeof(struct
sockaddr_storage));
```

Wrong Memory Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=745
Status	New

The function malloc in tcpdump/jni/tcpdump/addrtoname.c at line 633 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	646	646
Object	sizeof	malloc

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method isonsap_string(const u_char *nsap, register u_int nsap_length)

```
....
646.          tp->e_name = cp = (char
*)malloc(sizeof("xx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx"));
```

Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods 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 Methods\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=122
Status	New

The buffer allocated by sizeof in tcpdump/jni/libpcap/pcap-bpf.c at line 2317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	2335	2335
Object	ifm_name	sizeof

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method monitor_mode(pcap_t *p, int set)

```
....
2335.       strncpy(req.ifm_name, p->opt.source, sizeof req.ifm_name);
```

Client Use Of JQuery Outdated Version

Query Path:
JavaScript\Cx\JavaScript Medium Threat\Client Use Of JQuery Outdated Version Version:1

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities

Description
Client Use Of JQuery Outdated Version\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=158
Status	New

Method in tcpdump/jni/libpcap/tests/visopts.py, at line 54, calls an obsolete API, 2. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	tcpdump/jni/libpcap/tests/visopts.py	tcpdump/jni/libpcap/tests/visopts.py
Line	54	54
Object	2	2

Code Snippet
File Name tcpdump/jni/libpcap/tests/visopts.py

Method	<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"/></script>

```
....
54.      <script type="text/javascript"
src="http://ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"/>
</script>
```

Use of a One Way Hash without a Salt

Query Path:
CPP\Cx\CPP Medium Threat\Use of a One Way Hash without a Salt Version:1

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-13 Cryptographic Protection (P1)

Description
Use of a One Way Hash without a Salt\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=696
Status	New

The application protects passwords with MD5_Final in signature_compute_hmac_md5, of tcpdump/jni/tcpdump/signature.c at line 49, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	tcpdump/jni/tcpdump/signature.c	tcpdump/jni/tcpdump/signature.c
Line	63	65
Object	Address	MD5_Final

Code Snippet
File Name tcpdump/jni/tcpdump/signature.c
Method signature_compute_hmac_md5(const uint8_t *text, int text_len, unsigned char *key,

```
....
63.          MD5_Init(&tctx);
....
65.          MD5_Final(tk, &tctx);
```

Client Use Of JQuery Outdated Version

Query Path:
Typescript\Cx\Typescript Medium Threat\Client Use Of JQuery Outdated Version Version:1

Description
Client Use Of JQuery Outdated Version\Path 1:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=697
Status	New

Method in tcpdump/jni/libpcap/tests/visopts.py, at line 54, calls an obsolete API, 2. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	tcpdump/jni/libpcap/tests/visopts.py	tcpdump/jni/libpcap/tests/visopts.py
Line	54	54
Object	2	2

Code Snippet
File Name tcpdump/jni/libpcap/tests/visopts.py
Method <script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"/></script>

```
....
54.      <script type="text/javascript"
src="http://ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"/>
</script>
```

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=1000001&projectid=2&pathid=714
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/inet.c	tcpdump/jni/libpcap/inet.c
Line	185	421
Object	nextdev	nextdev

Code Snippet
File Name tcpdump/jni/libpcap/inet.c
Method add_or_find_if(pcap_if_t **curdev_ret, pcap_if_t **alldevs, const char *name,

```
....
185.        pcap_if_t *curdev, *prevdev, *nextdev;
....
421.              curdev->next = nextdev;
```

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=1000001&projectid=2&pathid=1098
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	1673	1698
Object	addr	sizeof

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method get_dlpi_ppa(register int fd, register const char *ifname, register int unit,

```
....
1673.       void *addr;
....
1698.           &addr, sizeof(addr), ebuf) < 0) {
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1099
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	485	490
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix4(netdissect_options *ndo,

```
....
485.                    const u_char *pptr, u_int itemlen, char *buf, u_int
buflen)
....
490.          ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1100
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	485	490
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix4(netdissect_options *ndo,

```
....
485.                    const u_char *pptr, u_int itemlen, char *buf, u_int
buflen)
....
490.          ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1101
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	485	490
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix4(netdissect_options *ndo,

```
....
485.                 const u_char *pptr, u_int itemlen, char *buf, u_int
buflen)
....
490.         ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1102
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	712	717
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_rt_routing_info(netdissect_options *ndo,

```
....
712.                         const u_char *pptr, char *buf, u_int
buflen)
....
717.         ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1103
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	712	717
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_rt_routing_info(netdissect_options *ndo,

```
....
712.                          const u_char *pptr, char *buf, u_int
buflen)
....
717.         ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1104
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	712	717
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_rt_routing_info(netdissect_options *ndo,

```
....
712.                          const u_char *pptr, char *buf, u_int
buflen)
....
717.         ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1105
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	752	757
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix4(netdissect_options *ndo,

```
....
752.                                const u_char *pptr, char *buf, u_int
buflen)
....
757.          ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1106
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	752	757
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix4(netdissect_options *ndo,

```
....
752.                                const u_char *pptr, char *buf, u_int
buflen)
....
757.          ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1107
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	752	757
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix4(netdissect_options *ndo,

```
....
752.                                const u_char *pptr, char *buf, u_int
buflen)
....
757.         ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1108
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	803	809
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_mdt_vpn_nlri(netdissect_options *ndo,

```
....
803.                        const u_char *pptr, char *buf, u_int buflen)
....
809.       ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1109
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	803	809
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_mdt_vpn_nlri(netdissect_options *ndo,

```
....
803.                        const u_char *pptr, char *buf, u_int buflen)
....
809.      ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1110
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	803	809
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_mdt_vpn_nlri(netdissect_options *ndo,

```
....
803.                        const u_char *pptr, char *buf, u_int buflen)
....
809.      ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1111
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	966	1026
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
966.                          const u_char *pptr, char *buf, u_int buflen)
....
1026.                    ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1112
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	966	1026
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
966.                        const u_char *pptr, char *buf, u_int buflen)
....
1026.                   ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1113
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	966	1026
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_l2(netdissect_options *ndo,

```
....
966.                        const u_char *pptr, char *buf, u_int buflen)
....
1026.                   ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=1114
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1060	1065
Object	pd	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix6(netdissect_options *ndo,

```
....
1060.                   const u_char *pd, u_int itemlen, char *buf, u_int
buflen)
....
1065.        ND_TCHECK(pd[0]);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1115
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1060	1065
Object	pd	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix6(netdissect_options *ndo,

```
....
1060.                   const u_char *pd, u_int itemlen, char *buf, u_int
buflen)
....
1065.        ND_TCHECK(pd[0]);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1116
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1060	1065
Object	pd	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix6(netdissect_options *ndo,

```
....
1060.                   const u_char *pd, u_int itemlen, char *buf, u_int
buflen)
....
1065.        ND_TCHECK(pd[0]);
```

Use of Sizeof On a Pointer Type\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1117
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1138	1143
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix6(netdissect_options *ndo,

```
....
1138.                               const u_char *pptr, char *buf, u_int
buflen)
....
1143.        ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1118
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c

Line	1138	1143
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix6(netdissect_options *ndo,

```
....
1138.                                const u_char *pptr, char *buf, u_int
buflen)
....
1143.        ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1119
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1138	1143
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix6(netdissect_options *ndo,

```
....
1138.                                const u_char *pptr, char *buf, u_int
buflen)
....
1143.        ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1120
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1178	1183
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_clnp_prefix(netdissect_options *ndo,

```
....
1178.                     const u_char *pptr, char *buf, u_int buflen)
....
1183.       ND_TCHECK(pptr[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=1000001&projectid=2&pathid=1121
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1178	1183
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_clnp_prefix(netdissect_options *ndo,

```
....
1178.                     const u_char *pptr, char *buf, u_int buflen)
....
1183.       ND_TCHECK(pptr[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=1000001&projectid=2&pathid=1122
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1178	1183
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_clnp_prefix(netdissect_options *ndo,

```
....
1178.                    const u_char *pptr, char *buf, u_int buflen)
....
1183.       ND_TCHECK(pptr[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=1000001&projectid=2&pathid=1123
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1208	1213
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_clnp_prefix(netdissect_options *ndo,

```
....
1208.                                const u_char *pptr, char *buf,
u_int buflen)
....
1213.       ND_TCHECK(pptr[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=1000001&projectid=2&pathid=1124
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1208	1213
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_clnp_prefix(netdissect_options *ndo,

```
....
1208.                                   const u_char *pptr, char *buf,
u_int buflen)
....
1213.       ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1125
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1208	1213
Object	pptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_clnp_prefix(netdissect_options *ndo,

```
....
1208.                                   const u_char *pptr, char *buf,
u_int buflen)
....
1213.       ND_TCHECK(pptr[0]);
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1126
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1256	1272
Object	tptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_attr_get_as_size(netdissect_options *ndo,

```
....
1256.       const u_char *tptr = pptr;
....
1272.           ND_TCHECK(tptr[0]);
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1127
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1256	1272
Object	tptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_attr_get_as_size(netdissect_options *ndo,

```
....
1256.       const u_char *tptr = pptr;
....
1272.           ND_TCHECK(tptr[0]);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1128
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1256	1272
Object	tptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_attr_get_as_size(netdissect_options *ndo,

```
....
1256.       const u_char *tptr = pptr;
....
1272.           ND_TCHECK(tptr[0]);
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1129
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1256	1280
Object	tptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_attr_get_as_size(netdissect_options *ndo,

```
....
1256.       const u_char *tptr = pptr;
....
1280.           ND_TCHECK(tptr[1]);
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1130
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1256	1280
Object	tptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_attr_get_as_size(netdissect_options *ndo,

```
....
1256.       const u_char *tptr = pptr;
....
1280.           ND_TCHECK(tptr[1]);
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=1131
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1256	1280
Object	tptr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_attr_get_as_size(netdissect_options *ndo,

```
....
1256.       const u_char *tptr = pptr;
....
1280.           ND_TCHECK(tptr[1]);
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1132
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	53
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
53.   ND_TCHECK(bp[0]);
```

Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1133
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	53
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
53.   ND_TCHECK(bp[0]);
```

Use of Sizeof On a Pointer Type\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1134
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	53
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
53.   ND_TCHECK(bp[0]);
```

Use of Sizeof On a Pointer Type\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1135
Status New

	Source	Destination

File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	65
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
65.   ND_TCHECK(bp[2]);
```

Use of Sizeof On a Pointer Type\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1136
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	65
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
65.   ND_TCHECK(bp[2]);
```

Use of Sizeof On a Pointer Type\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1137
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c

Line	48	65
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
65.   ND_TCHECK(bp[2]);
```

Use of Sizeof On a Pointer Type\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1138
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	66
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
66.   ND_TCHECK(bp[5]);
```

Use of Sizeof On a Pointer Type\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1139
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	66

Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
66.   ND_TCHECK(bp[5]);
```

Use of Sizeof On a Pointer Type\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1140
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-carp.c	tcpdump/jni/tcpdump/print-carp.c
Line	48	66
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-carp.c
Method carp_print(netdissect_options *ndo, register const u_char *bp, register u_int len, int ttl)

```
....
48.  carp_print(netdissect_options *ndo, register const u_char *bp,
register u_int len, int ttl)
....
66.   ND_TCHECK(bp[5]);
```

Use of Sizeof On a Pointer Type\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1141
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	69	78
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method dvmrp_print(netdissect_options *ndo,

```
....
69.              register const u_char *bp, register u_int len)
....
78.    ND_TCHECK(bp[1]);
```

Use of Sizeof On a Pointer Type\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1142
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	69	78
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method dvmrp_print(netdissect_options *ndo,

```
....
69.              register const u_char *bp, register u_int len)
....
78.    ND_TCHECK(bp[1]);
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1143
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	69	78
Object	bp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method dvmrp_print(netdissect_options *ndo,

```
....
69.              register const u_char *bp, register u_int len)
....
78.   ND_TCHECK(bp[1]);
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1144
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-eigrp.c	tcpdump/jni/tcpdump/print-eigrp.c
Line	211	268
Object	eigrp_tlv_header	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, register const u_char *pptr, register u_int len)

```
....
211.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
268.          ND_TCHECK2(*tptr, sizeof(struct eigrp_tlv_header));
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1145
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-eigrp.c	tcpdump/jni/tcpdump/print-eigrp.c
Line	211	268
Object	eigrp_tlv_header	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, register const u_char *pptr, register u_int len)

```
....
211.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
268.          ND_TCHECK2(*tptr, sizeof(struct eigrp_tlv_header));
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1146
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-eigrp.c	tcpdump/jni/tcpdump/print-eigrp.c
Line	211	268
Object	eigrp_tlv_header	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, register const u_char *pptr, register u_int len)

```
....
211.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
268.          ND_TCHECK2(*tptr, sizeof(struct eigrp_tlv_header));
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1147
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-eigrp.c	tcpdump/jni/tcpdump/print-eigrp.c
Line	211	275
Object	eigrp_tlv_header	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-eigrp.c
Method eigrp_print(netdissect_options *ndo, register const u_char *pptr, register u_int len)

```
....
211.      const struct eigrp_tlv_header *eigrp_tlv_header;
....
275.          if (eigrp_tlv_len < sizeof(struct eigrp_tlv_header) ||
```

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=1000001&projectid=2&pathid=753
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1091	1091
Object	fgets	fgets

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method linux_if_drops(const char * if_name)

```
....
1091.       while (!dropped_pkts && fgets( buffer, sizeof(buffer), file
))
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=754
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	2325	2325
Object	fgets	fgets

Code Snippet	
File Name	tcpdump/jni/libpcap/pcap-linux.c
Method	scan_proc_net_dev(pcap_if_t **devlistp, char *errbuf)

```
....
2325.           fgets(linebuf, sizeof linebuf, proc_net_f) != NULL;
linenum++) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=755
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getnetent.c	tcpdump/jni/libpcap/Win32/Src/getnetent.c
Line	66	66
Object	fgets	fgets

Code Snippet	
File Name	tcpdump/jni/libpcap/Win32/Src/getnetent.c
Method	getnetent()

```
....
66.   p = fgets(line, BUFSIZ, netf);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=756
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getservent.c	tcpdump/jni/libpcap/Win32/Src/getservent.c
Line	87	87
Object	fgets	fgets

Code Snippet	
File Name	tcpdump/jni/libpcap/Win32/Src/getservent.c
Method	getservent()

```
....
87.   if ((p = fgets(line, BUFSIZ, servf)) == NULL)
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=757
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	554	554
Object	fgets	fgets

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
554.              while (fgets(line, sizeof(line), fp)) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=758
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	444	444
Object	fgets	fgets

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
444.              while (fgets(fileline, sizeof(fileline)-1, secretfile)
!= NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=759
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	888	888
Object	fgets	fgets

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method get_next_file(FILE *VFile, char *ptr)

```
....
888.        ret = fgets(ptr, PATH_MAX, VFile);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=760
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	165	165
Object	fgets	fgets

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method static int init_ethers (void)

```
....
165.    while (fgets(buf,sizeof(buf),fp))
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=761
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/msdos/bin2c.c	tcpdump/jni/libpcap/msdos/bin2c.c

Line	34	34
Object	fgetc	fgetc

Code Snippet
File Name tcpdump/jni/libpcap/msdos/bin2c.c
Method int main (int argc, char **argv)

```
....
34.    while ((ch = fgetc(inFile)) != EOF)
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=762
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1091	1091
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method linux_if_drops(const char * if_name)

```
....
1091.       while (!dropped_pkts && fgets( buffer, sizeof(buffer), file
))
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=763
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	2325	2325
Object	linebuf	linebuf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method scan_proc_net_dev(pcap_if_t **devlistp, char *errbuf)

```
....
2325.           fgets(linebuf, sizeof linebuf, proc_net_f) != NULL;
linenum++) {
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=764
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getnetent.c	tcpdump/jni/libpcap/Win32/Src/getnetent.c
Line	66	66
Object	line	line

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getnetent.c
Method getnetent()

```
....
66.   p = fgets(line, BUFSIZ, netf);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=765
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getservent.c	tcpdump/jni/libpcap/Win32/Src/getservent.c
Line	87	87
Object	line	line

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getservent.c
Method getservent()

```
....
87.   if ((p = fgets(line, BUFSIZ, servf)) == NULL)
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=766
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	554	554
Object	line	line

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
554.              while (fgets(line, sizeof(line), fp)) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=767
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	444	444
Object	fileline	fileline

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
444.              while (fgets(fileline, sizeof(fileline)-1, secretfile)
!= NULL) {
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=768
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	888	888
Object	ptr	ptr

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method get_next_file(FILE *VFile, char *ptr)

```
....
888.        ret = fgets(ptr, PATH_MAX, VFile);
```

Improper Resource Access Authorization\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=769
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	165	165
Object	buf	buf

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method static int init_ethers (void)

```
....
165.    while (fgets(buf,sizeof(buf),fp))
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=770
Status New

	Source	Destination
File	tcpdump/jni/libpcap/savefile.c	tcpdump/jni/libpcap/savefile.c
Line	272	272
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/savefile.c
Method pcap_fopen_offline_with_tstamp_precision(FILE *fp, u_int precision,

```
....
272.        amt_read = fread((char *)&magic, 1, sizeof(magic), fp);
```

Improper Resource Access Authorization\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=771
Status New

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4076	4076
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static int yy_get_next_buffer (void)

```
....
4076.             YY_INPUT( (&YY_CURRENT_BUFFER_LVALUE-
>yy_ch_buf[number_to_move]),
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=772
Status New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	184	184
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_check_header(bpf_u_int32 magic, FILE *fp, u_int precision, char *errbuf,

```
....
184.        amt_read = fread(((char *)&hdr) + sizeof hdr.magic, 1,
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=773
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	412	412
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
412.        amt_read = fread(&sf_hdr, 1, ps->hdrsize, fp);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=774
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	521	521
Object	tp	tp

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
521.            amt_read = fread((char *)tp, 1, hdr->caplen, fp);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=775
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	546	546
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
546.              amt_read = fread(p->buffer, 1, hdr->caplen, fp);
```

Improper Resource Access Authorization\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=776
Status New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	732	732
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_dump_open_append(pcap_t *p, const char *fname)

```
....
732.        amt_read = fread(&ph, 1, sizeof (ph), f);
```

Improper Resource Access Authorization\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=777
Status New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	236	236
Object	buf	buf

Code Snippet

File Name	tcpdump/jni/libpcap/sf-pcap-ng.c
Method	read_bytes(FILE *fp, void *buf, size_t bytes_to_read, int fail_on_eof,

```
....
236.        amt_read = fread(buf, 1, bytes_to_read, fp);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=778
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	693	693
Object	Address	Address

Code Snippet

File Name	tcpdump/jni/libpcap/sf-pcap-ng.c
Method	pcap_ng_check_header(bpf_u_int32 magic, FILE *fp, u_int precision, char *errbuf,

```
....
693.        amt_read = fread(&total_length, 1, sizeof(total_length),
fp);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=779
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	709	709
Object	Address	Address

Code Snippet

File Name	tcpdump/jni/libpcap/sf-pcap-ng.c
Method	pcap_ng_check_header(bpf_u_int32 magic, FILE *fp, u_int precision, char *errbuf,

```
....
709.        amt_read = fread(&byte_order_magic, 1,
sizeof(byte_order_magic), fp);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=780
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	869	869
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_read_bpf(pcap_t *p, int cnt, pcap_handler callback, u_char *user)

```
....
869.                    cc = read(p->fd, (char *)p->buffer, p->bufsize);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=781
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-canusb-linux.c	tcpdump/jni/libpcap/pcap-canusb-linux.c
Line	403	403
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/pcap-canusb-linux.c
Method canusb_read_linux(pcap_t *handle, int max_packets, pcap_handler callback, u_char *user)

```
....
403.          n = read(handle->fd, &msg, sizeof(msg));
```

Improper Resource Access Authorization\Path 30:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=782
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	1730	1730
Object	buf	buf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method dlpi_kread(register int fd, register off_t addr,

```
....
1730.       cc = read(fd, buf, len);
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=783
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-nit.c	tcpdump/jni/libpcap/pcap-nit.c
Line	113	113
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-nit.c
Method pcap_read_nit(pcap_t *p, int cnt, pcap_handler callback, u_char *user)

```
....
113.              cc = read(p->fd, (char *)p->buffer, p->bufsize);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=784
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-pf.c	tcpdump/jni/libpcap/pcap-pf.c

Line	115	115
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name tcpdump/jni/libpcap/pcap-pf.c
Method pcap_read_pf(pcap_t *pc, int cnt, pcap_handler callback, u_char *user)

```
....
115.                cc = read(pc->fd, (char *)pc->buffer + pc->offset, pc->bufsize);
```

Improper Resource Access Authorization\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=785
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-snit.c	tcpdump/jni/libpcap/pcap-snit.c
Line	129	129
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snit.c
Method pcap_read_snit(pcap_t *p, int cnt, pcap_handler callback, u_char *user)

```
....
129.                cc = read(p->fd, (char *)p->buffer, p->bufsize);
```

Improper Resource Access Authorization\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=786
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-snoop.c	tcpdump/jni/libpcap/pcap-snoop.c
Line	87	87
Object	buffer	buffer

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snoop.c
Method pcap_read_snoop(pcap_t *p, int cnt, pcap_handler callback, u_char *user)

```
....
87.    cc = read(p->fd, (char *)p->buffer, p->bufsize);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=787
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	487	487
Object	line	line

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_read_linux(pcap_t *handle, int max_packets, pcap_handler callback, u_char *user)

```
....
487.                ret = read(handle->fd, line, USB_LINE_LEN - 1);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=788
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	706	706
Object	string	string

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_stats_linux(pcap_t *handle, struct pcap_stat *stats)

```
....
706.                ret = read(fd, string, USB_LINE_LEN-1);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=789
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/tests/filtertest.c	tcpdump/jni/libpcap/tests/filtertest.c
Line	92	92
Object	cp	cp

Code Snippet
File Name tcpdump/jni/libpcap/tests/filtertest.c
Method read_infile(char *fname)

```
....
92.    cc = read(fd, cp, (u_int)buf.st_size);
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=790
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/tests/valgrindtest.c	tcpdump/jni/libpcap/tests/valgrindtest.c
Line	120	120
Object	cp	cp

Code Snippet
File Name tcpdump/jni/libpcap/tests/valgrindtest.c
Method read_infile(char *fname)

```
....
120.        cc = read(fd, cp, (u_int)buf.st_size);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=791
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c

Line	560	560
Object	phydev_path	phydev_path

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method get_mac80211_phydev(pcap_t *handle, const char *device, char *phydev_path,

```
....
560.        bytes_read = readlink(pathstr, phydev_path,
phydev_max_pathlen);
```

Improper Resource Access Authorization\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=792
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-win32.c	tcpdump/jni/libpcap/pcap-win32.c
Line	719	719
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/pcap-win32.c
Method pcap_activate_win32(pcap_t *p)

```
....
719.                            &lptype,
```

Improper Resource Access Authorization\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=793
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-win32.c	tcpdump/jni/libpcap/pcap-win32.c
Line	720	720
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/pcap-win32.c
Method pcap_activate_win32(pcap_t *p)

```
....
720.                            (char*)&postype,
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=794
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-win32.c	tcpdump/jni/libpcap/pcap-win32.c
Line	721	721
Object	Address	Address

Code Snippet
File Name tcpdump/jni/libpcap/pcap-win32.c
Method pcap_activate_win32(pcap_t *p)

```
....
721.                            &lpcbdata);
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=795
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/msdos/bin2c.c	tcpdump/jni/libpcap/msdos/bin2c.c
Line	28	28
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/msdos/bin2c.c
Method int main (int argc, char **argv)

```
....
28.    fprintf (outFile,
```

Improper Resource Access Authorization\Path 44:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=796
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/msdos/bin2c.c	tcpdump/jni/libpcap/msdos/bin2c.c
Line	38	38
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/msdos/bin2c.c
Method int main (int argc, char **argv)

```
....
38.      fprintf (outFile, "0x%02X,", ch);
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=797
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2259	2259
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method dot_dump_node(struct block *block, struct bpf_program *prog, FILE *out)

```
....
2259.       fprintf(out, "\tblock%d [shape=ellipse, id=\"block-%d\"
label=\"BLOCK%d\\n", block->id, block->id, block->id);
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=798
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c

Line	2261	2261
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method dot_dump_node(struct block *block, struct bpf_program *prog, FILE *out)

```
....
2261.             fprintf(out, "\\n%s", bpf_image(prog->bf_insns + i,
i));
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=799
Status New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2263	2263
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method dot_dump_node(struct block *block, struct bpf_program *prog, FILE *out)

```
....
2263.       fprintf(out, "\" tooltip=\"");
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=800
Status New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2266	2266
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method dot_dump_node(struct block *block, struct bpf_program *prog, FILE *out)

```
....
2266.                   fprintf(out, "val[%d]=%d ", i, block->val[i]);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=801
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2267	2267
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method dot_dump_node(struct block *block, struct bpf_program *prog, FILE *out)

```
....
2267.       fprintf(out, "val[A]=%d ", block->val[A_ATOM]);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=802
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	2268	2268
Object	fprintf	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method dot_dump_node(struct block *block, struct bpf_program *prog, FILE *out)

```
....
2268.       fprintf(out, "val[X]=%d", block->val[X_ATOM]);
```

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=1000001&projectid=2&pathid=969
Status	New

The bpf_load method calls the sprintf function, at line 1166 of tcpdump/jni/libpcap/pcap-bpf.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	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1220	1220
Object	sprintf	sprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method bpf_load(char *errbuf)

```
....
1220.                    sprintf(buf, "%s%d", BPF_NODE, i);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=970
Status	New

The bpf_load method calls the sprintf function, at line 1166 of tcpdump/jni/libpcap/pcap-bpf.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	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1234	1234
Object	sprintf	sprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method bpf_load(char *errbuf)

```
....
1234.       sprintf(cfg_ld.path, "%s/%s", DRIVER_PATH, BPF_NAME);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=971
Status	New

The dlstrerror method calls the sprintf function, at line 1105 of tcpdump/jni/libpcap/pcap-dlpi.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	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	1209	1209
Object	sprintf	sprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method dlstrerror(bpf_u_int32 dl_errno)

```
....
1209.             sprintf(errstring, "Error %02x", dl_errno);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=972
Status	New

The dlprim method calls the sprintf function, at line 1215 of tcpdump/jni/libpcap/pcap-dlpi.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	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	1303	1303
Object	sprintf	sprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method dlprim(bpf_u_int32 prim)

```
....
1303.              (void) sprintf(primbuf, "unknown primitive 0x%x",
prim);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=973
Status	New

The *pcap_alloc method calls the malloc function, at line 4719 of tcpdump/jni/libpcap/scanner.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	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4721	4721
Object	malloc	malloc

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method void *pcap_alloc (yy_size_t size)

```
....
4721.       return (void *) malloc( size );
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=974
Status	New

The *pcap_realloc method calls the realloc function, at line 4724 of tcpdump/jni/libpcap/scanner.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	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4733	4733
Object	realloc	realloc

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method void *pcap_realloc (void * ptr, yy_size_t size)

```
....
4733.       return (void *) realloc( (char *) ptr, size );
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=975
Status	New

The *iptos method calls the sprintf function, at line 132 of tcpdump/jni/libpcap/tests/findalldevstest.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	tcpdump/jni/libpcap/tests/findalldevstest.c	tcpdump/jni/libpcap/tests/findalldevstest.c
Line	140	140
Object	sprintf	sprintf

Code Snippet
File Name tcpdump/jni/libpcap/tests/findalldevstest.c
Method static char *iptos(bpf_u_int32 in)

```
....
140.        sprintf(output[which], "%d.%d.%d.%d", p[0], p[1], p[2],
p[3]);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=976
Status	New

The ieee8021q_tci_string method calls the _snprintf function, at line 1221 of tcpdump/jni/tcpdump/addrtoname.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	1224	1224
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c

Method	ieee8021q_tci_string(const uint16_t tci)

```
....
1224.       snprintf(buf, sizeof(buf), "vlan %u, p %u%s",
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=977
Status	New

The etheraddr_string method calls the _snprintf function, at line 470 of tcpdump/jni/tcpdump/addrtoname.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	508	508
Object	_snprintf	_snprintf

Code Snippet	
File Name	tcpdump/jni/tcpdump/addrtoname.c
Method	etheraddr_string(netdissect_options *ndo, register const u_char *ep)

```
....
508.              snprintf(cp, BUFSIZE - (2 + 5*3), " (oui %s)",
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=978
Status	New

The tcpport_string method calls the _snprintf function, at line 663 of tcpdump/jni/tcpdump/addrtoname.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	676	676
Object	_snprintf	_snprintf

Code Snippet	
File Name	tcpdump/jni/tcpdump/addrtoname.c
Method	tcpport_string(u_short port)

```
....
676.        (void)snprintf(buf, sizeof(buf), "%u", i);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=979
Status	New

The udpport_string method calls the _snprintf function, at line 682 of tcpdump/jni/tcpdump/addrtoname.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	695	695
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method udpport_string(register u_short port)

```
....
695.        (void)snprintf(buf, sizeof(buf), "%u", i);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=980
Status	New

The init_servarray method calls the _snprintf function, at line 727 of tcpdump/jni/tcpdump/addrtoname.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	747	747
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method init_servarray(netdissect_options *ndo)

```
....
747.                    (void)snprintf(buf, sizeof(buf), "%d", port);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=981
Status	New

The getnameinfo method calls the snprintf function, at line 95 of tcpdump/jni/tcpdump/missing/getnameinfo.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	tcpdump/jni/tcpdump/missing/getnameinfo.c	tcpdump/jni/tcpdump/missing/getnameinfo.c
Line	157	157
Object	snprintf	snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/missing/getnameinfo.c
Method getnameinfo(sa, salen, host, hostlen, serv, servlen, flags)

```
....
157.                    snprintf(numserv, sizeof(numserv), "%d",
ntohs(port));
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=982
Status	New

The hex_and_ascii_print_with_offset method calls the _snprintf function, at line 93 of tcpdump/jni/tcpdump/print-ascii.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	tcpdump/jni/tcpdump/print-ascii.c	tcpdump/jni/tcpdump/print-ascii.c
Line	112	112
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-ascii.c

Method	hex_and_ascii_print_with_offset(netdissect_options *ndo, register const char *ident,

```
....
112.                (void)snprintf(hsp, sizeof(hexstuff) - (hsp -
hexstuff),
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=983
Status	New

The hex_and_ascii_print_with_offset method calls the _snprintf function, at line 93 of tcpdump/jni/tcpdump/print-ascii.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	tcpdump/jni/tcpdump/print-ascii.c	tcpdump/jni/tcpdump/print-ascii.c
Line	129	129
Object	_snprintf	_snprintf

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-ascii.c
Method	hex_and_ascii_print_with_offset(netdissect_options *ndo, register const char *ident,

```
....
129.                (void)snprintf(hsp, sizeof(hexstuff) - (hsp -
hexstuff),
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=984
Status	New

The ddpskt_string method calls the _snprintf function, at line 612 of tcpdump/jni/tcpdump/print-atalk.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	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	618	618
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ddpskt_string(netdissect_options *ndo,

```
....
618.                (void)snprintf(buf, sizeof(buf), "%d", skt);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=985
Status	New

The ataddr_string method calls the _snprintf function, at line 536 of tcpdump/jni/tcpdump/print-atalk.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	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	586	586
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
586.                    (void)snprintf(nambuf, sizeof(nambuf), "%s.%d",
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=986
Status	New

The ataddr_string method calls the _snprintf function, at line 536 of tcpdump/jni/tcpdump/print-atalk.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	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	595	595
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
595.                (void)snprintf(nambuf, sizeof(nambuf), "%d.%d", atnet,
athost);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=987
Status	New

The ataddr_string method calls the _snprintf function, at line 536 of tcpdump/jni/tcpdump/print-atalk.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	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	597	597
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
597.                (void)snprintf(nambuf, sizeof(nambuf), "%d", atnet);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=988
Status	New

The format_id method calls the _snprintf function, at line 107 of tcpdump/jni/tcpdump/print-babel.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	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	110	110
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_id(const u_char *id)

```
....
110.      snprintf(buf, 25, "%02x:%02x:%02x:%02x:%02x:%02x:%02x:%02x",
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=989
Status	New

The format_prefix method calls the _snprintf function, at line 120 of tcpdump/jni/tcpdump/print-babel.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	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	124	124
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_prefix(netdissect_options *ndo, const u_char *prefix, unsigned char plen)

```
....
124.          snprintf(buf, 50, "%s/%u", ipaddr_string(ndo, prefix +
12), plen - 96);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=990
Status	New

The format_prefix method calls the _snprintf function, at line 120 of tcpdump/jni/tcpdump/print-babel.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	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	127	127
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_prefix(netdissect_options *ndo, const u_char *prefix, unsigned char plen)

```
....
127.          snprintf(buf, 50, "%s/%u", ip6addr_string(ndo, prefix),
plen);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=991
Status	New

The format_interval method calls the _snprintf function, at line 149 of tcpdump/jni/tcpdump/print-babel.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	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	155	155
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_interval(const uint16_t i)

```
....
155.      snprintf(buf, sizeof(buf), "%u.%02us", i / 100, i % 100);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=992
Status	New

The format_timestamp method calls the _snprintf function, at line 166 of tcpdump/jni/tcpdump/print-babel.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	tcpdump/jni/tcpdump/print-babel.c	tcpdump/jni/tcpdump/print-babel.c
Line	169	169
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-babel.c
Method format_timestamp(const uint32_t i)

```
....
169.      snprintf(buf, sizeof(buf), "%u.%06us", i / 1000000, i %
1000000);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=993
Status	New

The as_printf method calls the _snprintf function, at line 470 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	474	474
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method as_printf(netdissect_options *ndo,

```
....
474.              snprintf(str, size, "%u", asnum);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=994
Status	New

The as_printf method calls the _snprintf function, at line 470 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	476	476
Object	_snprintf	_snprintf

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-bgp.c
Method	as_printf(netdissect_options *ndo,

```
....
476.                snprintf(str, size, "%u.%u", asnum >> 16, asnum &
0xFFFF);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=995
Status	New

The decode_prefix4 method calls the _snprintf function, at line 484 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	506	506
Object	_snprintf	_snprintf

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-bgp.c
Method	decode_prefix4(netdissect_options *ndo,

```
....
506.          snprintf(buf, buflen, "%s/%d", getname(ndo, (u_char
*)&addr), plen);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=996
Status	New

The decode_labeled_prefix4 method calls the _snprintf function, at line 517 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	555	555
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_prefix4(netdissect_options *ndo,

```
....
555.        snprintf(buf, buflen, "%s/%d, label:%u %s",
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=997
Status	New

The bgp_vpn_ip_print method calls the _snprintf function, at line 576 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	587	587
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_ip_print(netdissect_options *ndo,

```
....
587.          snprintf(pos, sizeof(addr), "%s", ipaddr_string(ndo,
pptr));
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=998
Status	New

The bgp_vpn_ip_print method calls the _snprintf function, at line 576 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	592	592
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_ip_print(netdissect_options *ndo,

```
....
592.            snprintf(pos, sizeof(addr), "%s", ip6addr_string(ndo,
pptr));
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=999
Status	New

The bgp_vpn_ip_print method calls the _snprintf function, at line 576 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	596	596
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_ip_print(netdissect_options *ndo,

```
....
596.            snprintf(pos, sizeof(addr), "bogus address length %u",
addr_length);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1000
Status	New

The bgp_vpn_sg_print method calls the _snprintf function, at line 625 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	642	642

Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_sg_print(netdissect_options *ndo,

```
....
642.          snprintf(buf + offset, buflen - offset, ", Source %s",
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1001
Status	New

The bgp_vpn_sg_print method calls the _snprintf function, at line 625 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	656	656
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_sg_print(netdissect_options *ndo,

```
....
656.          snprintf(buf + offset, buflen - offset, ", Group %s",
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1002
Status	New

The bgp_vpn_rd_print method calls the _snprintf function, at line 670 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	682	682

Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
682.          snprintf(pos, sizeof(rd) - (pos - rd), "%u:%u (=
%u.%u.%u.%u)",
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1003
Status	New

The bgp_vpn_rd_print method calls the _snprintf function, at line 670 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	690	690
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
690.          snprintf(pos, sizeof(rd) - (pos - rd), "%u.%u.%u.%u:%u",
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1004
Status	New

The bgp_vpn_rd_print method calls the _snprintf function, at line 670 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	696	696

Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
696.         snprintf(pos, sizeof(rd) - (pos - rd), "%s:%u
(%u.%u.%u.%u:%u)",
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1005
Status	New

The bgp_vpn_rd_print method calls the _snprintf function, at line 670 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	702	702
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method bgp_vpn_rd_print(netdissect_options *ndo,

```
....
702.           snprintf(pos, sizeof(rd) - (pos - rd), "unknown RD
format");
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1006
Status	New

The decode_rt_routing_info method calls the _snprintf function, at line 711 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c

Line	721	721
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_rt_routing_info(netdissect_options *ndo,

```
....
721.              snprintf(buf, buflen, "default route target");
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1007
Status	New

The decode_rt_routing_info method calls the _snprintf function, at line 711 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	740	740
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_rt_routing_info(netdissect_options *ndo,

```
....
740.        snprintf(buf, buflen, "origin AS: %s, route target %s",
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1008
Status	New

The decode_labeled_vpn_prefix4 method calls the _snprintf function, at line 751 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c

Line	776	776
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_prefix4(netdissect_options *ndo,

```
....
776.        snprintf(buf, buflen, "RD: %s, %s/%d, label:%u %s",
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1009
Status	New

The decode_mdt_vpn_nlri method calls the _snprintf function, at line 802 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	829	829
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_mdt_vpn_nlri(netdissect_options *ndo,

```
....
829.      snprintf(buf, buflen, "RD: %s, VPN IP Address: %s, MC Group
Address: %s",
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1010
Status	New

The decode_multicast_vpn method calls the _snprintf function, at line 858 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c

Line	868	868
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
868.          snprintf(buf, buflen, "Route-Type: %s (%u), length: %u",
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1011
Status	New

The decode_multicast_vpn method calls the _snprintf function, at line 858 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	877	877
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
877.              snprintf(buf + offset, buflen - offset, ", RD: %s,
Originator %s",
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1012
Status	New

The decode_multicast_vpn method calls the _snprintf function, at line 858 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c

Line	885	885
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
885.            snprintf(buf + offset, buflen - offset, ", RD: %s,
Source-AS %s",
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1013
Status	New

The decode_multicast_vpn method calls the _snprintf function, at line 858 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	894	894
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
894.              snprintf(buf + offset, buflen - offset, ", RD: %s",
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1014
Status	New

The decode_multicast_vpn method calls the _snprintf function, at line 858 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c

Line	903	903
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
903.              snprintf(buf + offset, buflen - offset, ", Originator
%s",
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1015
Status	New

The decode_multicast_vpn method calls the _snprintf function, at line 858 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	910	910
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
910.              snprintf(buf + offset, buflen - offset, ", RD: %s",
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1016
Status	New

The decode_multicast_vpn method calls the _snprintf function, at line 858 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c

Line	921	921
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_multicast_vpn(netdissect_options *ndo,

```
....
921.            snprintf(buf + offset, buflen - offset, ", RD: %s,
Source-AS %s",
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1017
Status	New

The decode_prefix6 method calls the _snprintf function, at line 1059 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1081	1081
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_prefix6(netdissect_options *ndo,

```
....
1081.       snprintf(buf, buflen, "%s/%d", getname6(ndo, (u_char
*)&addr), plen);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1018
Status	New

The decode_labeled_prefix6 method calls the _snprintf function, at line 1092 of tcpdump/jni/tcpdump/print-bgp.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	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1121	1121
Object	_snprintf	_snprintf

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_prefix6(netdissect_options *ndo,

```
....
1121.       snprintf(buf, buflen, "%s/%d, label:%u %s",
```

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=1000001&projectid=2&pathid=1415
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/missing/inet_ntop.c	tcpdump/jni/tcpdump/missing/inet_ntop.c
Line	121	121
Object	words	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/missing/inet_ntop.c
Method inet_ntop_v6 (const u_char *src, char *dst, size_t size)

```
....
121.    memset (words, 0, sizeof(words));
```

Sizeof Pointer Argument\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1416
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1189	1189

Object	addr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_clnp_prefix(netdissect_options *ndo,

```
....
1189.        memset(&addr, 0, sizeof(addr));
```

Sizeof Pointer Argument\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1417
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bgp.c	tcpdump/jni/tcpdump/print-bgp.c
Line	1224	1224
Object	addr	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-bgp.c
Method decode_labeled_vpn_clnp_prefix(netdissect_options *ndo,

```
....
1224.        memset(&addr, 0, sizeof(addr));
```

Sizeof Pointer Argument\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1418
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-nfs.c	tcpdump/jni/tcpdump/print-nfs.c
Line	471	471
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-nfs.c
Method parsefh(netdissect_options *ndo,

```
....
471.        if (ND_TTEST2(*dp, len * sizeof(*dp))) {
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1419
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-nfs.c	tcpdump/jni/tcpdump/print-nfs.c
Line	471	471
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-nfs.c
Method parsefh(netdissect_options *ndo,

```
....
471.        if (ND_TTEST2(*dp, len * sizeof(*dp))) {
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1420
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rx.c	tcpdump/jni/tcpdump/print-rx.c
Line	1643	1643
Object	s	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-rx.c
Method vldb_print(netdissect_options *ndo,

```
....
1643.                   VECOUT(VLNAMEMAX);
```

Sizeof Pointer Argument\Path 7:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1421
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rx.c	tcpdump/jni/tcpdump/print-rx.c
Line	1678	1678
Object	s	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-rx.c
Method vldb_print(netdissect_options *ndo,

```
....
1678.                    VECOUT(VLNAMEMAX);
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1422
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/util.c	tcpdump/jni/tcpdump/util.c
Line	480	480
Object	bitmasks	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/util.c
Method mask62plen(const u_char *mask)

```
....
480.              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=1000001&projectid=2&pathid=1423
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/util.c	tcpdump/jni/tcpdump/util.c

Line	480	480
Object	bitmasks	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/util.c
Method mask62plen(const u_char *mask)

```
....
480.              for (bits = 0; bits < (sizeof (bitmasks) / sizeof
(bitmasks[0])); bits++) {
```

Sizeof Pointer Argument\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1424
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.              ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1425
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.              ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1426
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.              ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1427
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-nfs.c	tcpdump/jni/tcpdump/print-nfs.c
Line	471	471
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-nfs.c
Method parsefh(netdissect_options *ndo,

```
....
471.          if (ND_TTEST2(*dp, len * sizeof(*dp))) {
```

Sizeof Pointer Argument\Path 14:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1428
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-nfs.c	tcpdump/jni/tcpdump/print-nfs.c
Line	826	826
Object	temp	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-nfs.c
Method nfs_printfh(netdissect_options *ndo,

```
....
826.                temp[sizeof(temp) - 1] = '\0';
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1429
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
....
205.                        ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1430
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c

Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
....
205.                        ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1431
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
....
205.                        ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1432
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	205
Object	Pointer	sizeof

Code Snippet

File Name	tcpdump/jni/tcpdump/print-dvmrp.c
Method	print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1433
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	205
Object	Pointer	sizeof

Code Snippet

File Name	tcpdump/jni/tcpdump/print-dvmrp.c
Method	print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1434
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	205
Object	Pointer	sizeof

Code Snippet

File Name	tcpdump/jni/tcpdump/print-dvmrp.c
Method	print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 21:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1435
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1436
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1437
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c

Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1438
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1439
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1440
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	243
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
```

Sizeof Pointer Argument\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1441
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	254
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
....
254.                      ND_TCHECK(cp[1]);
```

Sizeof Pointer Argument\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1442
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	254
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
....
254.                      ND_TCHECK(cp[1]);
```

Sizeof Pointer Argument\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1443
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	254
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
....
254.                      ND_TCHECK(cp[1]);
```

Sizeof Pointer Argument\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1444
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rx.c	tcpdump/jni/tcpdump/print-rx.c
Line	1555	1555
Object	s	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-rx.c
Method prot_reply_print(netdissect_options *ndo,

```
....
1555.                           VECOUT(PRNAMEMAX);
```

Sizeof Pointer Argument\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1445
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	288
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
....
288.                      ND_TCHECK(cp[3]);
```

Sizeof Pointer Argument\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1446
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	288
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
....
288.                      ND_TCHECK(cp[3]);
```

Sizeof Pointer Argument\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1447
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-ip.c	tcpdump/jni/tcpdump/print-ip.c
Line	243	288
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-ip.c
Method ip_optprint(netdissect_options *ndo,

```
....
243.                ND_TCHECK(*cp);
....
288.                      ND_TCHECK(cp[3]);
```

Sizeof Pointer Argument\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1448
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rx.c	tcpdump/jni/tcpdump/print-rx.c
Line	1089	1089
Object	a	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-rx.c
Method fs_reply_print(netdissect_options *ndo,

```
....
1089.                    acl_print(ndo, (u_char *) a, sizeof(a), (u_char
*) a + i);
```

Sizeof Pointer Argument\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1449
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rx.c	tcpdump/jni/tcpdump/print-rx.c
Line	2335	2335
Object	s	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-rx.c
Method vol_reply_print(netdissect_options *ndo,

```
....
2335.                                       VECOUT(32);
```

Sizeof Pointer Argument\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1450
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	1862	1862
Object	cmds	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method main(int argc, char **argv)

```
....
1862.                    sizeof(cmds) / sizeof(cmds[0])) < 0 && errno !=
ENOSYS) {
```

Sizeof Pointer Argument\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1451
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	199
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1452
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	199
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1453
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c

Line	199	199
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1454
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	199
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
205.                        ND_TCHECK(*bp);
....
199.                              ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1455
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	199
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
....
199.                          ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1456
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	199
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
....
199.                          ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1457
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                          ND_TCHECK(*bp);
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1458
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
....
205.                        ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1459
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
....
205.                        ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=1460
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1461
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1462
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	205	205

Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1463
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                        ND_TCHECK(*bp);
....
205.                    ND_TCHECK(*bp);
```

Sizeof Pointer Argument\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1464
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-dvmrp.c	tcpdump/jni/tcpdump/print-dvmrp.c
Line	199	205
Object	Pointer	sizeof

Code Snippet
File Name tcpdump/jni/tcpdump/print-dvmrp.c
Method print_report(netdissect_options *ndo,

```
....
199.                            ND_TCHECK(*bp);
....
205.                        ND_TCHECK(*bp);
```

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=1000001&projectid=2&pathid=1362
Status	New

The variable declared in null at tcpdump/jni/libpcap/gencode.c in line 430 is not initialized when it is used by s at tcpdump/jni/libpcap/gencode.c in line 430.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	465	505
Object	null	s

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method pcap_compile(pcap_t *p, struct bpf_program *program,

```
....
465.        root = NULL;
....
505.                    (root->s.code == (BPF_RET|BPF_K) && root->s.k ==
0))
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1363
Status	New

The variable declared in null at tcpdump/jni/libpcap/gencode.c in line 430 is not initialized when it is used by s at tcpdump/jni/libpcap/gencode.c in line 430.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	465	505
Object	null	s

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method pcap_compile(pcap_t *p, struct bpf_program *program,

```
....
465.        root = NULL;
....
505.                    (root->s.code == (BPF_RET|BPF_K) && root->s.k ==
0))
```

NULL Pointer Dereference\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1364
Status New

The variable declared in null at tcpdump/jni/libpcap/gencode.c in line 2595 is not initialized when it is used by next at tcpdump/jni/libpcap/gencode.c in line 6654.

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	2639	6661
Object	null	next

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method insert_compute_vloffsets(b)

```
....
2639.             s = NULL;
```

File Name tcpdump/jni/libpcap/gencode.c
Method sappend(s0, s1)

```
....
6661.       while (s0->next)
```

NULL Pointer Dereference\Path 4:

Severity Low
Result State To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1365
Status	New

The variable declared in null at tcpdump/jni/libpcap/scanner.c in line 3986 is not initialized when it is used by yy_buf_size at tcpdump/jni/libpcap/scanner.c in line 3986.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4039	4049
Object	null	yy_buf_size

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static int yy_get_next_buffer (void)

```
....
4039.                    YY_BUFFER_STATE b = YY_CURRENT_BUFFER;
....
4049.                                b->yy_buf_size += b->yy_buf_size /
8;
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1366
Status	New

The variable declared in null at tcpdump/jni/libpcap/scanner.c in line 3986 is not initialized when it is used by yy_buf_size at tcpdump/jni/libpcap/scanner.c in line 3986.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4039	4051
Object	null	yy_buf_size

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static int yy_get_next_buffer (void)

```
....
4039.                    YY_BUFFER_STATE b = YY_CURRENT_BUFFER;
....
4051.                                b->yy_buf_size *= 2;
```

NULL Pointer Dereference\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1367
Status	New

The variable declared in null at tcpdump/jni/libpcap/scanner.c in line 3986 is not initialized when it is used by yy_is_our_buffer at tcpdump/jni/libpcap/scanner.c in line 3986.

	Source	Destination
File	tcpdump/jni/libpcap/scanner.c	tcpdump/jni/libpcap/scanner.c
Line	4039	4044
Object	null	yy_is_our_buffer

Code Snippet
File Name tcpdump/jni/libpcap/scanner.c
Method static int yy_get_next_buffer (void)

```
....
4039.                    YY_BUFFER_STATE b = YY_CURRENT_BUFFER;
....
4044.                    if ( b->yy_is_our_buffer )
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1368
Status	New

The variable declared in null at tcpdump/jni/tcpdump/print-udp.c in line 292 is not initialized when it is used by ip6_ctlun at tcpdump/jni/tcpdump/print-udp.c in line 292.

	Source	Destination
File	tcpdump/jni/tcpdump/print-udp.c	tcpdump/jni/tcpdump/print-udp.c
Line	300	303
Object	null	ip6_ctlun

Code Snippet
File Name tcpdump/jni/tcpdump/print-udp.c
Method udpipaddr_print(netdissect_options *ndo, const struct ip *ip, int sport, int dport)

```
....
300.                ip6 = NULL;
....
303.                if (ip6->ip6_nxt == IPPROTO_UDP) {
```

NULL Pointer Dereference\Path 8:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1369
Status	New

The variable declared in 0 at tcpdump/jni/libpcap/pcap-linux.c in line 3833 is not initialized when it is used by tp_retire_blk_tov at tcpdump/jni/libpcap/pcap-linux.c in line 3833.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	4121	4121
Object	0	tp_retire_blk_tov

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method create_ring(pcap_t *handle, int *status)

```
....
4121.        req.tp_retire_blk_tov = (handlep->timeout>=0)?handlep-
>timeout:0;
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1370
Status	New

The variable declared in 0 at tcpdump/jni/tcpdump/print-udp.c in line 194 is not initialized when it is used by rr_dv at tcpdump/jni/tcpdump/print-udp.c in line 194.

	Source	Destination
File	tcpdump/jni/tcpdump/print-udp.c	tcpdump/jni/tcpdump/print-udp.c
Line	197	266
Object	0	rr_dv

Code Snippet
File Name tcpdump/jni/tcpdump/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
197.        struct rtcp_rr *rr = 0;
....
266.              ND_PRINT((ndo, " %ul %us %uj @%.2f+%.2f",
```

NULL Pointer Dereference\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1371
Status	New

The variable declared in 0 at tcpdump/jni/tcpdump/print-udp.c in line 194 is not initialized when it is used by rr_ls at tcpdump/jni/tcpdump/print-udp.c in line 194.

	Source	Destination
File	tcpdump/jni/tcpdump/print-udp.c	tcpdump/jni/tcpdump/print-udp.c
Line	197	266
Object	0	rr_ls

Code Snippet
File Name tcpdump/jni/tcpdump/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
197.        struct rtcp_rr *rr = 0;
....
266.              ND_PRINT((ndo, " %ul %us %uj @%.2f+%.2f",
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1372
Status	New

The variable declared in 0 at tcpdump/jni/tcpdump/print-udp.c in line 194 is not initialized when it is used by rr_nl at tcpdump/jni/tcpdump/print-udp.c in line 194.

	Source	Destination
File	tcpdump/jni/tcpdump/print-udp.c	tcpdump/jni/tcpdump/print-udp.c
Line	197	266
Object	0	rr_nl

Code Snippet
File Name tcpdump/jni/tcpdump/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
197.        struct rtcp_rr *rr = 0;
....
266.              ND_PRINT((ndo, " %ul %us %uj @%.2f+%.2f",
```

NULL Pointer Dereference\Path 12:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1373
Status	New

The variable declared in 0 at tcpdump/jni/tcpdump/print-udp.c in line 194 is not initialized when it is used by rr_srcid at tcpdump/jni/tcpdump/print-udp.c in line 194.

	Source	Destination
File	tcpdump/jni/tcpdump/print-udp.c	tcpdump/jni/tcpdump/print-udp.c
Line	197	263
Object	0	rr_srcid

Code Snippet
File Name tcpdump/jni/tcpdump/print-udp.c
Method rtcp_print(netdissect_options *ndo, const u_char *hdr, const u_char *ep)

```
....
197.        struct rtcp_rr *rr = 0;
....
263.                    ND_PRINT((ndo, " %u", EXTRACT_32BITS(&rr-
>rr_srcid)));
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1374
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by namelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	346	362
Object	gabn	namelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
346.              lwres_gabnrequest_t *gabn;
....
362.                    s = (const char *)&gabn->namelen +
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1375
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by namelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	346	360
Object	gabn	namelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
346.              lwres_gabnrequest_t *gabn;
....
360.                    ND_TCHECK(gabn->namelen);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1376
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by namelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	346	364
Object	gabn	namelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
346.              lwres_gabnrequest_t *gabn;
....
364.                    l = EXTRACT_16BITS(&gabn->namelen);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1377
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by flags at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	346	368
Object	gabn	flags

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
346.              lwres_gabnrequest_t *gabn;
....
368.                              ND_PRINT((ndo, " flags:0x%x",
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1378
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by addrtypes at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	346	372
Object	gabn	addrtypes

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
346.              lwres_gabnrequest_t *gabn;
....
372.                    v = EXTRACT_32BITS(&gabn->addrtypes);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1379
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by flags at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	347	398
Object	gnba	flags

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
347.              lwres_gnbarequest_t *gnba;
....
398.                              ND_PRINT((ndo, " flags:0x%x",
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1380
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by addr at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	347	394
Object	gnba	addr

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
347.              lwres_gnbarequest_t *gnba;
....
394.                    ND_TCHECK(gnba->addr);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1381
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by addr at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	347	402
Object	gnba	addr

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
347.              lwres_gnbarequest_t *gnba;
....
402.                    s = (const char *)&gnba->addr;
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1382
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by addr at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	347	404
Object	gnba	addr

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
347.              lwres_gnbarequest_t *gnba;
....
404.                    advance = lwres_printaddr(ndo, &gnba->addr);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1383
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by flags at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	348	416
Object	grbn	flags

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
348.              lwres_grbnrequest_t *grbn;
....
416.                              ND_PRINT((ndo, " flags:0x%x",
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1384
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by namelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	348	412
Object	grbn	namelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
348.              lwres_grbnrequest_t *grbn;
....
412.                    ND_TCHECK(grbn->namelen);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1385
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by rdtype at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	348	420
Object	grbn	rdtype

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
348.              lwres_grbnrequest_t *grbn;
....
420.                    ND_PRINT((ndo, " %s", tok2str(ns_type2str,
"Type%d",
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1386
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by rdclass at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	348	422
Object	grbn	rdclass

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
348.              lwres_grbnrequest_t *grbn;
....
422.                    if (EXTRACT_16BITS(&grbn->rdclass) != C_IN) {
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1387
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by rdclass at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	348	423
Object	grbn	rdclass

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
348.              lwres_grbnrequest_t *grbn;
....
423.                              ND_PRINT((ndo, " %s",
tok2str(ns_class2str, "Class%d",
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1388
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by namelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	348	428
Object	grbn	namelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
348.              lwres_grbnrequest_t *grbn;
....
428.                    s = (const char *)&grbn->namelen +
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1389
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by namelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	348	430
Object	grbn	namelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
348.              lwres_grbnrequest_t *grbn;
....
430.                    l = EXTRACT_16BITS(&grbn->namelen);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1390
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by realnamelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	462
Object	gabn	realnamelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
445.              lwres_gabnresponse_t *gabn;
....
462.                    s = (const char *)&gabn->realnamelen +
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1391
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by realnamelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	460
Object	gabn	realnamelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
445.              lwres_gabnresponse_t *gabn;
....
460.                    ND_TCHECK(gabn->realnamelen);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1392
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by realnamelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	464
Object	gabn	realnamelen

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
445.              lwres_gabnresponse_t *gabn;
....
464.                    l = EXTRACT_16BITS(&gabn->realnamelen);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1393
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by flags at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	468
Object	gabn	flags

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
445.              lwres_gabnresponse_t *gabn;
....
468.                           ND_PRINT((ndo, " flags:0x%x",
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1394
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by naliases at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	472
Object	gabn	naliases

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
445.              lwres_gabnresponse_t *gabn;
....
472.                    ND_PRINT((ndo, " %u/%u", EXTRACT_16BITS(&gabn-
>naliases),
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1395
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by naddrs at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	472
Object	gabn	naddrs

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
445.              lwres_gabnresponse_t *gabn;
....
472.                    ND_PRINT((ndo, " %u/%u", EXTRACT_16BITS(&gabn-
>naliases),
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1396
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by naliases at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	481
Object	gabn	naliases

Code Snippet

File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
445.                lwres_gabnresponse_t *gabn;
....
481.                      na = EXTRACT_16BITS(&gabn->naliases);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1397
Status	New

The variable declared in gabn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by naddrs at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	445	490
Object	gabn	naddrs

Code Snippet

File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
445.                lwres_gabnresponse_t *gabn;
....
490.                      na = EXTRACT_16BITS(&gabn->naddrs);
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1398
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by realnamelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	446	502
Object	gnba	realnamelen

Code Snippet

File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
446.                lwres_gnbaresponse_t *gnba;
....
502.                      s = (const char *)&gnba->realnamelen +
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1399
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by realnamelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	446	500
Object	gnba	realnamelen

Code Snippet

File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
446.                lwres_gnbaresponse_t *gnba;
....
500.                      ND_TCHECK(gnba->realnamelen);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1400
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by realnamelen at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	446	504
Object	gnba	realnamelen

Code Snippet

File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
446.                lwres_gnbaresponse_t *gnba;
....
504.                      l = EXTRACT_16BITS(&gnba->realnamelen);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1401
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by flags at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	446	508
Object	gnba	flags

Code Snippet

File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
446.                lwres_gnbaresponse_t *gnba;
....
508.                            ND_PRINT((ndo, " flags:0x%x",
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1402
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by naliases at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	446	512
Object	gnba	naliases

Code Snippet

File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
446.              lwres_gnbaresponse_t *gnba;
....
512.                    ND_PRINT((ndo, " %u", EXTRACT_16BITS(&gnba-
>naliases)));
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1403
Status	New

The variable declared in gnba at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by naliases at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	446	520
Object	gnba	naliases

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-lwres.c
Method	lwres_print(netdissect_options *ndo,

```
....
446.              lwres_gnbaresponse_t *gnba;
....
520.                    na = EXTRACT_16BITS(&gnba->naliases);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1404
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by flags at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	535
Object	grbn	flags

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
535.                           ND_PRINT((ndo, " flags:0x%x",
```

NULL Pointer Dereference\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1405
Status New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by nsigs at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	531
Object	grbn	nsigs

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
531.                    ND_TCHECK(grbn->nsigs);
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1406
Status New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by rdtype at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	539
Object	grbn	rdtype

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
539.                    ND_PRINT((ndo, " %s", tok2str(ns_type2str,
"Type%d",
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1407
Status New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by rdclass at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	541
Object	grbn	rdclass

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
541.                    if (EXTRACT_16BITS(&grbn->rdclass) != C_IN) {
```

NULL Pointer Dereference\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1408
Status New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by rdclass at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	542
Object	grbn	rdclass

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
542.                           ND_PRINT((ndo, " %s",
tok2str(ns_class2str, "Class%d",
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1409
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by ttl at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	546
Object	grbn	ttl

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
546.                    relts_print(ndo, EXTRACT_32BITS(&grbn->ttl));
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1410
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by nrdatas at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	547

Object	grbn	nrdatas

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
547.                    ND_PRINT((ndo, " %u/%u", EXTRACT_16BITS(&grbn-
>nrdatas),
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1411
Status	New

The variable declared in grbn at tcpdump/jni/tcpdump/print-lwres.c in line 293 is not initialized when it is used by nsigs at tcpdump/jni/tcpdump/print-lwres.c in line 293.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lwres.c	tcpdump/jni/tcpdump/print-lwres.c
Line	447	547
Object	grbn	nsigs

Code Snippet
File Name tcpdump/jni/tcpdump/print-lwres.c
Method lwres_print(netdissect_options *ndo,

```
....
447.              lwres_grbnresponse_t *grbn;
....
547.                    ND_PRINT((ndo, " %u/%u", EXTRACT_16BITS(&grbn-
>nrdatas),
```

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=1000001&projectid=2&pathid=1519
Status	New

The main method in tcpdump/jni/libpcap/msdos/bin2c.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	tcpdump/jni/libpcap/msdos/bin2c.c	tcpdump/jni/libpcap/msdos/bin2c.c
Line	25	25
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/msdos/bin2c.c
Method int main (int argc, char **argv)

```
....
25.    if ((inFile = fopen(argv[1],"rb")) == NULL)
```

TOCTOU\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1520
Status New

The pcap_ether_hostton method in tcpdump/jni/libpcap/nametoaddr.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	tcpdump/jni/libpcap/nametoaddr.c	tcpdump/jni/libpcap/nametoaddr.c
Line	441	441
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/nametoaddr.c
Method pcap_ether_hostton(const char *name)

```
....
441.                fp = fopen(PCAP_ETHERS_FILE, "r");
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1521
Status New

The linux_if_drops method in tcpdump/jni/libpcap/pcap-linux.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	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1087	1087
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method linux_if_drops(const char * if_name)

```
....
1087.       file = fopen("/proc/net/dev", "r");
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1522
Status New

The scan_proc_net_dev method in tcpdump/jni/libpcap/pcap-linux.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	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	2297	2297
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method scan_proc_net_dev(pcap_if_t **devlistp, char *errbuf)

```
....
2297.       proc_net_f = fopen("/proc/net/dev", "r");
```

TOCTOU\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1523
Status New

The pcap_open_offline_with_tstamp_precision method in tcpdump/jni/libpcap/savefile.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	tcpdump/jni/libpcap/savefile.c	tcpdump/jni/libpcap/savefile.c
Line	188	188
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/savefile.c
Method pcap_open_offline_with_tstamp_precision(const char *fname, u_int precision,

```
....
188.                fp = fopen(fname, "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1524
Status	New

The pcap_dump_open method in tcpdump/jni/libpcap/sf-pcap.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	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	667	667
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_dump_open(pcap_t *p, const char *fname)

```
....
667.                f = fopen(fname, "w");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1525
Status	New

The pcap_dump_open_append method in tcpdump/jni/libpcap/sf-pcap.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	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	719	719
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_dump_open_append(pcap_t *p, const char *fname)

```
....
719.         f = fopen(fname, "r+");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1526
Status	New

The setnetent method in tcpdump/jni/libpcap/Win32/Src/getnetent.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	tcpdump/jni/libpcap/Win32/Src/getnetent.c	tcpdump/jni/libpcap/Win32/Src/getnetent.c
Line	41	41
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getnetent.c
Method setnetent(f)

```
....
41.          netf = fopen(NETDB, "r" );
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1527
Status	New

The getnetent method in tcpdump/jni/libpcap/Win32/Src/getnetent.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	tcpdump/jni/libpcap/Win32/Src/getnetent.c	tcpdump/jni/libpcap/Win32/Src/getnetent.c
Line	63	63
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getnetent.c
Method getnetent()

```
....
63.   if (netf == NULL && (netf = fopen(NETDB, "r" )) == NULL)
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1528
Status	New

The getservent method in tcpdump/jni/libpcap/Win32/Src/getservent.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	tcpdump/jni/libpcap/Win32/Src/getservent.c	tcpdump/jni/libpcap/Win32/Src/getservent.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getservent.c
Method getservent()

```
....
84.   if (servf == NULL && (servf = fopen(SERVDB, "r" )) == NULL)
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1529
Status	New

The setservent method in tcpdump/jni/libpcap/Win32/Src/getservent.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	tcpdump/jni/libpcap/Win32/Src/getservent.c	tcpdump/jni/libpcap/Win32/Src/getservent.c
Line	62	62
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getservent.c
Method setservent(f)

```
....
62.         servf = fopen(SERVDB, "r" );
```

TOCTOU\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1530
Status New

The ataddr_string method in tcpdump/jni/tcpdump/print-atalk.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	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	550	550
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/tcpdump/print-atalk.c
Method ataddr_string(netdissect_options *ndo,

```
....
550.             && (fp = fopen("/etc/atalk.names", "r"))) {
```

TOCTOU\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1531
Status New

The esp_print_decode_onesecret method in tcpdump/jni/tcpdump/print-esp.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	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	438	438
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
438.                secretfile = fopen(filename, FOPEN_READ_TXT);
```

TOCTOU\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1532
Status New

The main method in tcpdump/jni/tcpdump/tcpdump.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	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	1551	1551
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method main(int argc, char **argv)

```
....
1551.                           VFile = fopen(VFileName, "r");
```

TOCTOU\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1533
Status New

The init_ethers method in tcpdump/jni/tcpdump/win32/Src/ether_ntohost.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	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	160	160
Object	fopen	fopen

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method static int init_ethers (void)

```
....
160.    FILE *fp = fopen (etc_path("ethers"), "r");
```

TOCTOU\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1534
Status New

The bpf_open method in tcpdump/jni/libpcap/pcap-bpf.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	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	461	461
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method bpf_open(pcap_t *p)

```
....
461.        if ((fd = open(device, O_RDWR)) == -1 &&
```

TOCTOU\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1535
Status New

The bpf_open method in tcpdump/jni/libpcap/pcap-bpf.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	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c

Line	462	462
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method bpf_open(pcap_t *p)

```
....
462.            (errno != EACCES || (fd = open(device, O_RDONLY)) == -
1)) {
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1536
Status	New

The pcap_activate_dlpi method in tcpdump/jni/libpcap/pcap-dlpi.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	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	393	393
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method pcap_activate_dlpi(pcap_t *p)

```
....
393.        if ((p->fd = open(cp, O_RDWR)) < 0) {
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1537
Status	New

The pcap_activate_dlpi method in tcpdump/jni/libpcap/pcap-dlpi.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	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c

Line	415	415
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method pcap_activate_dlpi(pcap_t *p)

```
....
415.        pd->send_fd = open(cp, O_RDWR);
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1538
Status	New

The pcap_platform_finddevs method in tcpdump/jni/libpcap/pcap-dlpi.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	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c
Line	979	979
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method pcap_platform_finddevs(pcap_if_t **alldevsp, char *errbuf)

```
....
979.        if ((fd = open("/dev/ba", O_RDWR)) < 0) {
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1539
Status	New

The get_dlpi_ppa method in tcpdump/jni/libpcap/pcap-dlpi.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	tcpdump/jni/libpcap/pcap-dlpi.c	tcpdump/jni/libpcap/pcap-dlpi.c

Line	1691	1691
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dlpi.c
Method get_dlpi_ppa(register int fd, register const char *ifname, register int unit,

```
....
1691.        kd = open("/dev/kmem", O_RDONLY);
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1540
Status	New

The pcap_activate_snit method in tcpdump/jni/libpcap/pcap-snit.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	tcpdump/jni/libpcap/pcap-snit.c	tcpdump/jni/libpcap/pcap-snit.c
Line	319	319
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snit.c
Method pcap_activate_snit(pcap_t *p)

```
....
319.         p->fd = fd = open(dev, O_RDWR);
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1541
Status	New

The pcap_activate_snit method in tcpdump/jni/libpcap/pcap-snit.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	tcpdump/jni/libpcap/pcap-snit.c	tcpdump/jni/libpcap/pcap-snit.c

Line	321	321
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-snit.c
Method pcap_activate_snit(pcap_t *p)

```
....
321.                p->fd = fd = open(dev, O_RDONLY);
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1542
Status	New

The probe_devices method in tcpdump/jni/libpcap/pcap-usb-linux.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	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	264	264
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method probe_devices(int bus)

```
....
264.                fd = open(buf, O_RDWR);
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1543
Status	New

The usb_activate method in tcpdump/jni/libpcap/pcap-usb-linux.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	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c

Line	367	367
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_activate(pcap_t* handle)

```
....
367.        handle->fd = open(full_path, O_RDONLY, 0);
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1544
Status	New

The usb_activate method in tcpdump/jni/libpcap/pcap-usb-linux.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	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	406	406
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_activate(pcap_t* handle)

```
....
406.              handle->fd = open(full_path, O_RDONLY, 0);
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1545
Status	New

The usb_activate method in tcpdump/jni/libpcap/pcap-usb-linux.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	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c

Line	416	416
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_activate(pcap_t* handle)

```
....
416.                            handle->fd = open(full_path, O_RDONLY, 0);
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1546
Status	New

The usb_stats_linux method in tcpdump/jni/libpcap/pcap-usb-linux.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	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	684	684
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_stats_linux(pcap_t *handle, struct pcap_stat *stats)

```
....
684.        fd = open(string, O_RDONLY, 0);
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1547
Status	New

The usb_stats_linux method in tcpdump/jni/libpcap/pcap-usb-linux.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	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c

Line	694	694
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_stats_linux(pcap_t *handle, struct pcap_stat *stats)

```
....
694.                    fd = open(string, O_RDONLY, 0);
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1548
Status	New

The read_infile method in tcpdump/jni/libpcap/tests/filtertest.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	tcpdump/jni/libpcap/tests/filtertest.c	tcpdump/jni/libpcap/tests/filtertest.c
Line	81	81
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/tests/filtertest.c
Method read_infile(char *fname)

```
....
81.    fd = open(fname, O_RDONLY|O_BINARY);
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1549
Status	New

The read_infile method in tcpdump/jni/libpcap/tests/valgrindtest.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	tcpdump/jni/libpcap/tests/valgrindtest.c	tcpdump/jni/libpcap/tests/valgrindtest.c

Line	109	109
Object	open	open

Code Snippet
File Name tcpdump/jni/libpcap/tests/valgrindtest.c
Method read_infile(char *fname)

```
....
109.        fd = open(fname, O_RDONLY|O_BINARY);
```

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=1000001&projectid=2&pathid=935
Status	New

The system data read by void perror in the file tcpdump/jni/libpcap/lbl/os-sunos4.h at line 126 is potentially exposed by void perror found in tcpdump/jni/libpcap/lbl/os-sunos4.h at line 126.

	Source	Destination
File	tcpdump/jni/libpcap/lbl/os-sunos4.h	tcpdump/jni/libpcap/lbl/os-sunos4.h
Line	126	126
Object	perror	perror

Code Snippet
File Name tcpdump/jni/libpcap/lbl/os-sunos4.h
Method void perror(const char *);

```
....
126.  void  perror(const char *);
```

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=1000001&projectid=2&pathid=936
Status	New

The system data read by void perror in the file tcpdump/jni/tcpdump/lbl/os-sunos4.h at line 126 is potentially exposed by void perror found in tcpdump/jni/tcpdump/lbl/os-sunos4.h at line 126.

	Source	Destination
File	tcpdump/jni/tcpdump/lbl/os-sunos4.h	tcpdump/jni/tcpdump/lbl/os-sunos4.h
Line	126	126
Object	perror	perror

Code Snippet
File Name tcpdump/jni/tcpdump/lbl/os-sunos4.h
Method void perror(const char *);

```
....
126.  void  perror(const char *);
```

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=1000001&projectid=2&pathid=937
Status	New

The system data read by esp_print_decode_onesecret in the file tcpdump/jni/tcpdump/print-esp.c at line 406 is potentially exposed by esp_print_decode_onesecret found in tcpdump/jni/tcpdump/print-esp.c at line 406.

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	440	440
Object	perror	perror

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
440.                    perror(filename);
```

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=1000001&projectid=2&pathid=938
Status	New

The system data read by pcap_cleanup_bpf in the file tcpdump/jni/libpcap/pcap-bpf.c at line 1271 is potentially exposed by pcap_cleanup_bpf found in tcpdump/jni/libpcap/pcap-bpf.c at line 1271.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1300	1297
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_cleanup_bpf(pcap_t *p)

```
....
1300.                                strerror(errno));
....
1297.                           fprintf(stderr,
```

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=1000001&projectid=2&pathid=939
Status New

The system data read by pcap_cleanup_bpf in the file tcpdump/jni/libpcap/pcap-bpf.c at line 1271 is potentially exposed by pcap_cleanup_bpf found in tcpdump/jni/libpcap/pcap-bpf.c at line 1271.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1309	1306
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_cleanup_bpf(pcap_t *p)

```
....
1309.                                    strerror(errno));
....
1306.                                fprintf(stderr,
```

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=1000001&projectid=2&pathid=940
Status New

The system data read by pcap_cleanup_bpf in the file tcpdump/jni/libpcap/pcap-bpf.c at line 1271 is potentially exposed by pcap_cleanup_bpf found in tcpdump/jni/libpcap/pcap-bpf.c at line 1271.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1327	1324
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method pcap_cleanup_bpf(pcap_t *p)

```
....
1327.                                                   strerror(errno));
....
1324.                                                fprintf(stderr,
```

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=1000001&projectid=2&pathid=941
Status	New

The system data read by canusb_capture_thread in the file tcpdump/jni/libpcap/pcap-canusb-linux.c at line 258 is potentially exposed by canusb_capture_thread found in tcpdump/jni/libpcap/pcap-canusb-linux.c at line 258.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-canusb-linux.c	tcpdump/jni/libpcap/pcap-canusb-linux.c
Line	282	282
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-canusb-linux.c
Method static void* canusb_capture_thread(void *arg)

```
....
282.                 fprintf(stderr,"write() error: %s\n",
strerror(errno));
```

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=1000001&projectid=2&pathid=942
Status	New

The system data read by dag_platform_cleanup in the file tcpdump/jni/libpcap/pcap-dag.c at line 145 is potentially exposed by dag_platform_cleanup found in tcpdump/jni/libpcap/pcap-dag.c at line 145.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	153	153
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_platform_cleanup(pcap_t *p)

```
....
153.                    fprintf(stderr,"dag_stop_stream: %s\n",
strerror(errno));
```

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=1000001&projectid=2&pathid=943
Status New

The system data read by dag_platform_cleanup in the file tcpdump/jni/libpcap/pcap-dag.c at line 145 is potentially exposed by dag_platform_cleanup found in tcpdump/jni/libpcap/pcap-dag.c at line 145.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	156	156
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_platform_cleanup(pcap_t *p)

```
....
156.                    fprintf(stderr,"dag_detach_stream: %s\n",
strerror(errno));
```

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=1000001&projectid=2&pathid=944
Status New

The system data read by dag_platform_cleanup in the file tcpdump/jni/libpcap/pcap-dag.c at line 145 is potentially exposed by dag_platform_cleanup found in tcpdump/jni/libpcap/pcap-dag.c at line 145.

	Source	Destination

File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	153	156
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_platform_cleanup(pcap_t *p)

```
....
153.                    fprintf(stderr,"dag_stop_stream: %s\n",
strerror(errno));
....
156.                    fprintf(stderr,"dag_detach_stream: %s\n",
strerror(errno));
```

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=1000001&projectid=2&pathid=945
Status New

The system data read by dag_platform_cleanup in the file tcpdump/jni/libpcap/pcap-dag.c at line 145 is potentially exposed by dag_platform_cleanup found in tcpdump/jni/libpcap/pcap-dag.c at line 145.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	163	163
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_platform_cleanup(pcap_t *p)

```
....
163.                        fprintf(stderr,"dag_close: %s\n",
strerror(errno));
```

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=1000001&projectid=2&pathid=946
Status New

The system data read by dag_platform_cleanup in the file tcpdump/jni/libpcap/pcap-dag.c at line 145 is potentially exposed by dag_platform_cleanup found in tcpdump/jni/libpcap/pcap-dag.c at line 145.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	153	163
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_platform_cleanup(pcap_t *p)

```
....
153.                    fprintf(stderr,"dag_stop_stream: %s\n",
strerror(errno));
....
163.                          fprintf(stderr,"dag_close: %s\n",
strerror(errno));
```

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=1000001&projectid=2&pathid=947
Status New

The system data read by dag_platform_cleanup in the file tcpdump/jni/libpcap/pcap-dag.c at line 145 is potentially exposed by dag_platform_cleanup found in tcpdump/jni/libpcap/pcap-dag.c at line 145.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-dag.c	tcpdump/jni/libpcap/pcap-dag.c
Line	156	163
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-dag.c
Method dag_platform_cleanup(pcap_t *p)

```
....
156.                    fprintf(stderr,"dag_detach_stream: %s\n",
strerror(errno));
....
163.                          fprintf(stderr,"dag_close: %s\n",
strerror(errno));
```

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=1000001&projectid=2&pathid=948
Status New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1179	1175
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1179.                                handlep->device, strerror(errno));
....
1175.                           fprintf(stderr,
```

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=1000001&projectid=2&pathid=949
Status New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1194	1189
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1194.                                        strerror(errno));
....
1189.                                   fprintf(stderr,
```

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=1000001&projectid=2&pathid=950
Status New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1260	1257
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1260.                               handlep->device, strerror(errno));
....
1257.                           fprintf(stderr,
```

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=1000001&projectid=2&pathid=951
Status New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1179	1257
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1179.                               handlep->device, strerror(errno));
....
1257.                           fprintf(stderr,
```

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=1000001&projectid=2&pathid=952
Status New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1194	1257
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1194.                                                strerror(errno));
....
1257.                           fprintf(stderr,
```

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=1000001&projectid=2&pathid=953
Status New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1273	1270
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1273.                                    handlep->device,
strerror(errno));
....
1270.                                 fprintf(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=1000001&projectid=2&pathid=954

Status	New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1179	1270
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1179.                                handlep->device, strerror(errno));
....
1270.                                  fprintf(stderr,
```

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=1000001&projectid=2&pathid=955
Status	New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1194	1270
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1194.                                          strerror(errno));
....
1270.                                fprintf(stderr,
```

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=1000001&projectid=2&pathid=956

Status	New

The system data read by void pcap_cleanup_linux in the file tcpdump/jni/libpcap/pcap-linux.c at line 1143 is potentially exposed by void pcap_cleanup_linux found in tcpdump/jni/libpcap/pcap-linux.c at line 1143.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1260	1270
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method static void pcap_cleanup_linux(pcap_t *handle)

```
....
1260.                                handlep->device, strerror(errno));
....
1270.                                  fprintf(stderr,
```

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=1000001&projectid=2&pathid=957
Status	New

The system data read by pcap_setfilter_linux_common in the file tcpdump/jni/libpcap/pcap-linux.c at line 2412 is potentially exposed by pcap_setfilter_linux_common found in tcpdump/jni/libpcap/pcap-linux.c at line 2412.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	2547	2545
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method pcap_setfilter_linux_common(pcap_t *handle, struct bpf_program *filter,

```
....
2547.                                    pcap_strerror(errno));
....
2545.                              fprintf(stderr,
```

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=1000001&projectid=2&pathid=958

Status	New

The system data read by enter_rfmon_mode_wext in the file tcpdump/jni/libpcap/pcap-linux.c at line 5164 is potentially exposed by enter_rfmon_mode_wext found in tcpdump/jni/libpcap/pcap-linux.c at line 5164.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5755	5752
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5755.                                strerror(errno));
....
5752.                             fprintf(stderr,
```

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=1000001&projectid=2&pathid=959
Status	New

The system data read by enter_rfmon_mode_wext in the file tcpdump/jni/libpcap/pcap-linux.c at line 5164 is potentially exposed by enter_rfmon_mode_wext found in tcpdump/jni/libpcap/pcap-linux.c at line 5164.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5742	5752
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method enter_rfmon_mode_wext(pcap_t *handle, int sock_fd, const char *device)

```
....
5742.                           "%s: Can't set flags: %s", device,
strerror(errno));
....
5752.                             fprintf(stderr,
```

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=1000001&projectid=2&p

	athid=960
Status	New

The system data read by droproot in the file tcpdump/jni/tcpdump/tcpdump.c at line 738 is potentially exposed by droproot found in tcpdump/jni/tcpdump/tcpdump.c at line 738.

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	752	751
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method droproot(const char *username, const char *chroot_dir)

```
....
752.                                chroot_dir, pcap_strerror(errno));
....
751.                            fprintf(stderr, "tcpdump: Couldn't
chroot/chdir to '%.64s': %s\n",
```

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=1000001&projectid=2&pathid=961
Status	New

The system data read by compress_savefile in the file tcpdump/jni/tcpdump/tcpdump.c at line 2182 is potentially exposed by compress_savefile found in tcpdump/jni/tcpdump/tcpdump.c at line 2182.

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	2203	2199
Object	errno	fprintf

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method compress_savefile(const char *filename)

```
....
2203.                    strerror(errno));
....
2199.              fprintf(stderr,
```

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=1000001&projectid=2&pathid=1493
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/gencode.c	tcpdump/jni/libpcap/gencode.c
Line	7095	7095
Object	n	n

Code Snippet
File Name tcpdump/jni/libpcap/gencode.c
Method free_reg(n)

```
....
7095.       regused[n] = 0;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1494
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/grammar.c	tcpdump/jni/libpcap/grammar.c
Line	1770	1770
Object	yyn	yyn

Code Snippet
File Name tcpdump/jni/libpcap/grammar.c
Method yytnamerr (char *yyres, const char *yystr)

```
....
1770.              yyres[yyn] = *yyp;
```

Unchecked Array Index\Path 3:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1495
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/grammar.c	tcpdump/jni/libpcap/grammar.c
Line	1776	1776
Object	yyn	yyn

Code Snippet
File Name tcpdump/jni/libpcap/grammar.c
Method yytnamerr (char *yyres, const char *yystr)

```
....
1776.             yyres[yyn] = '\0';
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1496
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	207	207
Object	level	level

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method find_levels_r(struct block *b)

```
....
207.        levels[level] = b;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1497
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	249	249

Object	dom	dom

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method find_dom(struct block *root)

```
....
249.                    SET_INSERT(b->dom, b->id);
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1498
Status New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	261	261
Object	edom	edom

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method propedom(struct edge *ep)

```
....
261.        SET_INSERT(ep->edom, ep->id);
```

Unchecked Array Index\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1499
Status New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	316	316
Object	closure	closure

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method find_closure(struct block *root)

```
....
316.                    SET_INSERT(b->closure, b->id);
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1500
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	564	564
Object	hash	hash

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method F(int code, int v0, int v1)

```
....
564.        hashtbl[hash] = p;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1501
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	1865	1865
Object	n	n

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method number_blks_r(struct block *p)

```
....
1865.       blocks[n] = p;
```

Unchecked Array Index\Path 10:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1502
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	2573	2573
Object	j	j

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method remove_en(pcap_t *p)

```
....
2573.             p->dlt_list[j] = p->dlt_list[i];
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1503
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	2620	2620
Object	j	j

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method remove_802_11(pcap_t *p)

```
....
2620.             p->dlt_list[j] = p->dlt_list[i];
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1504
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-canusb-linux.c	tcpdump/jni/libpcap/pcap-canusb-linux.c
Line	126	126

Object	n	n

Code Snippet
File Name tcpdump/jni/libpcap/pcap-canusb-linux.c
Method int canusb_findalldevs(pcap_if_t **alldevsp, char *err_str)

```
....
126.                sernum[n] = 0;
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1505
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-canusb-linux.c	tcpdump/jni/libpcap/pcap-canusb-linux.c
Line	170	170
Object	n	n

Code Snippet
File Name tcpdump/jni/libpcap/pcap-canusb-linux.c
Method static libusb_device_handle* canusb_opendevice(struct libusb_context *ctx, char* devserial)

```
....
170.            serial[n] = 0;
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1506
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	5900	5900
Object	j	j

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method iface_ethtool_get_ts_info(pcap_t *handle, char *ebuf)

```
....
5900.                           handle->tstamp_type_list[j] =
sof_ts_type_map[i].pcap_tstamp_val;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1507
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/missing/getopt_long.c	tcpdump/jni/tcpdump/missing/getopt_long.c
Line	165	165
Object	cstart	cstart

Code Snippet
File Name tcpdump/jni/tcpdump/missing/getopt_long.c
Method permute_args(int panonopt_start, int panonopt_end, int opt_end,

```
....
165.                    ((char **)nargv)[cstart] = swap;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1508
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-bootp.c	tcpdump/jni/tcpdump/print-bootp.c
Line	1085	1085
Object	i	i

Code Snippet
File Name tcpdump/jni/tcpdump/print-bootp.c
Method client_fqdn_flags(u_int flags)

```
....
1085.       buf[i] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1509
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	240	240
Object	i	i

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method int espprint_decode_hex(netdissect_options *ndo,

```
....
240.              binbuf[i] = hex2byte(ndo, hex);
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1510
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rpki-rtr.c	tcpdump/jni/tcpdump/print-rpki-rtr.c
Line	133	133
Object	idx	idx

Code Snippet
File Name tcpdump/jni/tcpdump/print-rpki-rtr.c
Method indent_string (u_int indent)

```
....
133.      buf[idx] = '\0';
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1511
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rpki-rtr.c	tcpdump/jni/tcpdump/print-rpki-rtr.c

Line	145	145
Object	idx	idx

Code Snippet
File Name tcpdump/jni/tcpdump/print-rpki-rtr.c
Method indent_string (u_int indent)

```
....
145.      buf[idx] = '\n';
```

Unchecked Array Index\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1512
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rpki-rtr.c	tcpdump/jni/tcpdump/print-rpki-rtr.c
Line	149	149
Object	idx	idx

Code Snippet
File Name tcpdump/jni/tcpdump/print-rpki-rtr.c
Method indent_string (u_int indent)

```
....
149.        buf[idx] = '\t';
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1513
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rpki-rtr.c	tcpdump/jni/tcpdump/print-rpki-rtr.c
Line	155	155
Object	idx	idx

Code Snippet
File Name tcpdump/jni/tcpdump/print-rpki-rtr.c
Method indent_string (u_int indent)

```
....
155.        buf[idx] = ' ';
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1514
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-rpki-rtr.c	tcpdump/jni/tcpdump/print-rpki-rtr.c
Line	163	163
Object	idx	idx

Code Snippet
File Name tcpdump/jni/tcpdump/print-rpki-rtr.c
Method indent_string (u_int indent)

```
....
163.      buf[idx] = '\0';
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1515
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-sl.c	tcpdump/jni/tcpdump/print-sl.c
Line	246	246
Object	lastconn	lastconn

Code Snippet
File Name tcpdump/jni/tcpdump/print-sl.c
Method compressed_sl_print(netdissect_options *ndo,

```
....
246.        lastlen[dir][lastconn] = length - (hlen << 2);
```

Unchecked Array Index\Path 24:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1516
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-sl.c	tcpdump/jni/tcpdump/print-sl.c
Line	153	153
Object	lastconn	lastconn

Code Snippet
File Name tcpdump/jni/tcpdump/print-sl.c
Method sliplink_print(netdissect_options *ndo,

```
....
153.              lastlen[dir][lastconn] = length - (hlen << 2);
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1517
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-sl.c	tcpdump/jni/tcpdump/print-sl.c
Line	246	246
Object	dir	dir

Code Snippet
File Name tcpdump/jni/tcpdump/print-sl.c
Method compressed_sl_print(netdissect_options *ndo,

```
....
246.        lastlen[dir][lastconn] = length - (hlen << 2);
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1518
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-sl.c	tcpdump/jni/tcpdump/print-sl.c
Line	153	153

Object	dir	dir

Code Snippet
File Name tcpdump/jni/tcpdump/print-sl.c
Method sliplink_print(netdissect_options *ndo,

```
....
153.              lastlen[dir][lastconn] = length - (hlen << 2);
```

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=1000001&projectid=2&pathid=920
Status New

	Source	Destination
File	tcpdump/jni/libpcap/msdos/bin2c.c	tcpdump/jni/libpcap/msdos/bin2c.c
Line	25	25
Object	inFile	inFile

Code Snippet
File Name tcpdump/jni/libpcap/msdos/bin2c.c
Method int main (int argc, char **argv)

```
....
25.    if ((inFile = fopen(argv[1],"rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=921
Status New

	Source	Destination
File	tcpdump/jni/libpcap/nametoaddr.c	tcpdump/jni/libpcap/nametoaddr.c

Line	441	441
Object	fp	fp

Code Snippet
File Name tcpdump/jni/libpcap/nametoaddr.c
Method pcap_ether_hostton(const char *name)

```
....
441.                fp = fopen(PCAP_ETHERS_FILE, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=922
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	1087	1087
Object	file	file

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method linux_if_drops(const char * if_name)

```
....
1087.       file = fopen("/proc/net/dev", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=923
Status New

	Source	Destination
File	tcpdump/jni/libpcap/pcap-linux.c	tcpdump/jni/libpcap/pcap-linux.c
Line	2297	2297
Object	proc_net_f	proc_net_f

Code Snippet
File Name tcpdump/jni/libpcap/pcap-linux.c
Method scan_proc_net_dev(pcap_if_t **devlistp, char *errbuf)

```
....
2297.       proc_net_f = fopen("/proc/net/dev", "r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=924
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/savefile.c	tcpdump/jni/libpcap/savefile.c
Line	188	188
Object	fp	fp

Code Snippet
File Name tcpdump/jni/libpcap/savefile.c
Method pcap_open_offline_with_tstamp_precision(const char *fname, u_int precision,

```
....
188.              fp = fopen(fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=925
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	667	667
Object	f	f

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_dump_open(pcap_t *p, const char *fname)

```
....
667.              f = fopen(fname, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=926
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	719	719
Object	f	f

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_dump_open_append(pcap_t *p, const char *fname)

```
....
719.         f = fopen(fname, "r+");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=927
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getnetent.c	tcpdump/jni/libpcap/Win32/Src/getnetent.c
Line	41	41
Object	netf	netf

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getnetent.c
Method setnetent(f)

```
....
41.          netf = fopen(NETDB, "r" );
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=928
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getnetent.c	tcpdump/jni/libpcap/Win32/Src/getnetent.c

Line	63	63
Object	netf	netf

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getnetent.c
Method getnetent()

```
....
63.   if (netf == NULL && (netf = fopen(NETDB, "r" )) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=929
Status New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getservent.c	tcpdump/jni/libpcap/Win32/Src/getservent.c
Line	84	84
Object	servf	servf

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getservent.c
Method getservent()

```
....
84.   if (servf == NULL && (servf = fopen(SERVDB, "r" )) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=930
Status New

	Source	Destination
File	tcpdump/jni/libpcap/Win32/Src/getservent.c	tcpdump/jni/libpcap/Win32/Src/getservent.c
Line	62	62
Object	servf	servf

Code Snippet
File Name tcpdump/jni/libpcap/Win32/Src/getservent.c

Method	setservent(f)

```
....
62.         servf = fopen(SERVDB, "r" );
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=931
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-atalk.c	tcpdump/jni/tcpdump/print-atalk.c
Line	550	550
Object	fp	fp

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-atalk.c
Method	ataddr_string(netdissect_options *ndo,

```
....
550.            && (fp = fopen("/etc/atalk.names", "r"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=932
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	438	438
Object	secretfile	secretfile

Code Snippet	
File Name	tcpdump/jni/tcpdump/print-esp.c
Method	static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
438.             secretfile = fopen(filename, FOPEN_READ_TXT);
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=933
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	1551	1551
Object	VFile	VFile

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method main(int argc, char **argv)

```
....
1551.                           VFile = fopen(VFileName, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=934
Status	New

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	160	160
Object	fp	fp

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method static int init_ethers (void)

```
....
160.    FILE *fp = fopen (etc_path("ethers"), "r");
```

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=1000001&projectid=2&pathid=708
Status	New

The size of the buffer used by usb_read_linux in "%x %d %c %c%c:%d:%d %s%n", at line 468 of tcpdump/jni/libpcap/pcap-usb-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that usb_read_linux passes to "%x %d %c %c%c:%d:%d %s%n", at line 468 of tcpdump/jni/libpcap/pcap-usb-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	507	507
Object	"%x %d %c %c%c:%d:%d %s%n"	"%x %d %c %c%c:%d:%d %s%n"

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_read_linux(pcap_t *handle, int max_packets, pcap_handler callback, u_char *user)

```
....
507.         ret = sscanf(string, "%x %d %c %c%c:%d:%d %s%n", &tag,
&timestamp, &etype,
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=709
Status	New

The size of the buffer used by usb_read_linux in "%s %s %s %s %s%n", at line 468 of tcpdump/jni/libpcap/pcap-usb-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that usb_read_linux passes to "%s %s %s %s %s%n", at line 468 of tcpdump/jni/libpcap/pcap-usb-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	574	574
Object	"%s %s %s %s %s%n"	"%s %s %s %s %s%n"

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_read_linux(pcap_t *handle, int max_packets, pcap_handler callback, u_char *user)

```
....
574.                 ret = sscanf(string, "%s %s %s %s %s%n", str1, str2,
str3, str4,
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=710
Status	New

The size of the buffer used by usb_stats_linux in "%s%n", at line 674 of tcpdump/jni/libpcap/pcap-usb-linux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that usb_stats_linux passes to "%s%n", at line 674 of tcpdump/jni/libpcap/pcap-usb-linux.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-usb-linux.c	tcpdump/jni/libpcap/pcap-usb-linux.c
Line	729	729
Object	"%s%n"	"%s%n"

Code Snippet
File Name tcpdump/jni/libpcap/pcap-usb-linux.c
Method usb_stats_linux(pcap_t *handle, struct pcap_stat *stats)

```
....
729.              ntok = sscanf(ptr, "%s%n", token, &cnt);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=711
Status	New

The size of the buffer used by bpf_load in "%s%d", at line 1166 of tcpdump/jni/libpcap/pcap-bpf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bpf_load passes to "%s%d", at line 1166 of tcpdump/jni/libpcap/pcap-bpf.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1220	1220
Object	"%s%d"	"%s%d"

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method bpf_load(char *errbuf)

```
....
1220.                  sprintf(buf, "%s%d", BPF_NODE, i);
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=712
Status	New

The size of the buffer used by bpf_load in "%s/%s", at line 1166 of tcpdump/jni/libpcap/pcap-bpf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bpf_load passes to "%s/%s", at line 1166 of tcpdump/jni/libpcap/pcap-bpf.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/pcap-bpf.c	tcpdump/jni/libpcap/pcap-bpf.c
Line	1234	1234
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name tcpdump/jni/libpcap/pcap-bpf.c
Method bpf_load(char *errbuf)

```
....
1234.       sprintf(cfg_ld.path, "%s/%s", DRIVER_PATH, BPF_NAME);
```

Potential Path Traversal

Query Path:
CPP\Cx\CPP Low Visibility\Potential Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description

Potential Path Traversal\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=962
Status	New

Method main at line 15 of tcpdump/jni/libpcap/msdos/bin2c.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 15 of tcpdump/jni/libpcap/msdos/bin2c.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	tcpdump/jni/libpcap/msdos/bin2c.c	tcpdump/jni/libpcap/msdos/bin2c.c
Line	15	25
Object	argv	argv

Code Snippet

File Name	tcpdump/jni/libpcap/msdos/bin2c.c
Method	int main (int argc, char **argv)

```
....
15.  int main (int argc, char **argv)
....
25.    if ((inFile = fopen(argv[1],"rb")) == NULL)
```

Potential Path Traversal\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=963
Status	New

Method *etc_path at line 81 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in init_ethers at line 157 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	84	160
Object	getenv	etc_path

Code Snippet

File Name	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method	const char *etc_path (const char *file)

```
....
84.    const char *env = win9x ? getenv("WinDir") :
getenv("SystemRoot");
```

File Name	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method	static int init_ethers (void)

```
....
160.    FILE *fp = fopen (etc_path("ethers"), "r");
```

Potential Path Traversal\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=964
Status	New

Method *etc_path at line 81 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in init_ethers at line 157 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	84	160
Object	getenv	etc_path

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method const char *etc_path (const char *file)

```
....
84.    const char *env = win9x ? getenv("WinDir") :
getenv("SystemRoot");
```

File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method static int init_ethers (void)

```
....
160.    FILE *fp = fopen (etc_path("ethers"), "r");
```

Potential Path Traversal\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=965
Status	New

Method *etc_path at line 81 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in init_ethers at line 157 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	84	160
Object	getenv	etc_path

Code Snippet
File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Method const char *etc_path (const char *file)

```
....
84.    const char *env = win9x ? getenv("WinDir") :
getenv("SystemRoot");
```

File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c

Method static int init_ethers (void)

```
....
160.    FILE *fp = fopen (etc_path("ethers"), "r");
```

Potential Path Traversal\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=966
Status	New

Method *etc_path at line 81 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in init_ethers at line 157 of tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c	tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c
Line	84	160
Object	getenv	etc_path

Code Snippet

File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c

Method const char *etc_path (const char *file)

```
....
84.    const char *env = win9x ? getenv("WinDir") :
getenv("SystemRoot");
```

File Name tcpdump/jni/tcpdump/win32/Src/ether_ntohost.c

Method static int init_ethers (void)

```
....
160.    FILE *fp = fopen (etc_path("ethers"), "r");
```

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=1000001&projectid=2&pathid=1357
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 102 of tcpdump/jni/tcpdump/addrtoname.c. The application then makes a security decision, dotp, in tcpdump/jni/tcpdump/addrtoname.c line 222, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	112	254
Object	gethostbyaddr	dotp

Code Snippet

File Name tcpdump/jni/tcpdump/addrtoname.c

Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
112.              return gethostbyaddr(addr, len, type);
```

File Name tcpdump/jni/tcpdump/addrtoname.c

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

```
....
254.                          if (dotp)
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1358
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 102 of tcpdump/jni/tcpdump/addrtoname.c. The application then makes a security decision, hp, in tcpdump/jni/tcpdump/addrtoname.c line 222, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	112	247
Object	gethostbyaddr	hp

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
112.                return gethostbyaddr(addr, len, type);
```

File Name tcpdump/jni/tcpdump/addrtoname.c
Method getname(netdissect_options *ndo, const u_char *ap)

```
....
247.                if (hp) {
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1359
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 102 of tcpdump/jni/tcpdump/addrtoname.c. The application then makes a security decision, dotp, in tcpdump/jni/tcpdump/addrtoname.c line 270, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	112	305
Object	gethostbyaddr	dotp

Code Snippet
File Name tcpdump/jni/tcpdump/addrtoname.c
Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
112.                return gethostbyaddr(addr, len, type);
```

File Name tcpdump/jni/tcpdump/addrtoname.c
Method getname6(netdissect_options *ndo, const u_char *ap)

```
....
305.                        if (dotp)
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1360
Status	New

The win32_gethostbyaddr method performs a reverse DNS lookup with gethostbyaddr, at line 102 of tcpdump/jni/tcpdump/addrtoname.c. The application then makes a security decision, hp, in tcpdump/jni/tcpdump/addrtoname.c line 270, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	tcpdump/jni/tcpdump/addrtoname.c	tcpdump/jni/tcpdump/addrtoname.c
Line	112	298
Object	gethostbyaddr	hp

Code Snippet

File Name tcpdump/jni/tcpdump/addrtoname.c

Method win32_gethostbyaddr(const char *addr, int len, int type)

```
....
112.              return gethostbyaddr(addr, len, type);
```

File Name tcpdump/jni/tcpdump/addrtoname.c

Method getname6(netdissect_options *ndo, const u_char *ap)

```
....
298.              if (hp) {
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1361
Status	New

The pcap_nametoaddrinfo method performs a reverse DNS lookup with getaddrinfo, at line 119 of tcpdump/jni/libpcap/nametoaddr.c. The application then makes a security decision, error, in tcpdump/jni/libpcap/nametoaddr.c line 119, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	tcpdump/jni/libpcap/nametoaddr.c	tcpdump/jni/libpcap/nametoaddr.c
Line	128	129
Object	getaddrinfo	error

Code Snippet
File Name tcpdump/jni/libpcap/nametoaddr.c
Method pcap_nametoaddrinfo(const char *name)

```
....
128.        error = getaddrinfo(name, NULL, &hints, &res);
129.        if (error)
```

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=1000001&projectid=2&pathid=701
Status	New

The buffer allocated by <= in tcpdump/jni/tcpdump/print-802_11.c at line 2819 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tcpdump/jni/tcpdump/print-802_11.c	tcpdump/jni/tcpdump/print-802_11.c
Line	2877	2877
Object	<=	<=

Code Snippet
File Name tcpdump/jni/tcpdump/print-802_11.c
Method ieee802_11_radio_print(netdissect_options *ndo,

```
....
2877.       for (bit0 = 0, presentp = &hdr->it_present; presentp <=
last_presentp;
```

Potential Off by One Error in Loops\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=702
Status	New

The buffer allocated by <= in tcpdump/jni/tcpdump/print-lldp.c at line 1104 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lldp.c	tcpdump/jni/tcpdump/print-lldp.c
Line	1188	1188
Object	<=	<=

Code Snippet
File Name tcpdump/jni/tcpdump/print-lldp.c
Method lldp_private_dcbx_print(netdissect_options *ndo,

```
....
1188.           for (i = 0; i <= 7; 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=1000001&projectid=2&pathid=703
Status	New

The buffer allocated by <= in tcpdump/jni/tcpdump/print-lldp.c at line 1104 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lldp.c	tcpdump/jni/tcpdump/print-lldp.c
Line	1193	1193
Object	<=	<=

Code Snippet
File Name tcpdump/jni/tcpdump/print-lldp.c
Method lldp_private_dcbx_print(netdissect_options *ndo,

```
....
1193.           for (i = 0; i <= 7; i++)
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=704
Status	New

The buffer allocated by <= in tcpdump/jni/tcpdump/print-lldp.c at line 1104 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tcpdump/jni/tcpdump/print-lldp.c	tcpdump/jni/tcpdump/print-lldp.c
Line	1214	1214
Object	<=	<=

Code Snippet
File Name tcpdump/jni/tcpdump/print-lldp.c
Method lldp_private_dcbx_print(netdissect_options *ndo,

```
....
1214.            for (i = 0; i <= 7; i++)
```

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=1000001&projectid=2&pathid=698
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/tests/filtertest.c	tcpdump/jni/libpcap/tests/filtertest.c
Line	220	220
Object	getopt	getopt

Code Snippet
File Name tcpdump/jni/libpcap/tests/filtertest.c
Method main(int argc, char **argv)

```
....
220.        while ((op = getopt(argc, argv, "dF:m:Os:")) != -1) {
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=699
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/tests/valgrindtest.c	tcpdump/jni/libpcap/tests/valgrindtest.c
Line	241	241
Object	getopt	getopt

Code Snippet
File Name tcpdump/jni/libpcap/tests/valgrindtest.c
Method main(int argc, char **argv)

```
....
241.        while ((op = getopt(argc, argv, "aF:i:I")) != -1) {
```

Inconsistent Implementations\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=700
Status New

	Source	Destination
File	tcpdump/jni/tcpdump/tcpdump.c	tcpdump/jni/tcpdump/tcpdump.c
Line	1076	1076
Object	getopt_long	getopt_long

Code Snippet
File Name tcpdump/jni/tcpdump/tcpdump.c
Method main(int argc, char **argv)

```
....
1076.           (op = getopt_long(argc, argv, SHORTOPTS, longopts,
NULL)) != -1)
```

Heuristic 2nd Order Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow malloc Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow malloc\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&p

	athid=706
Status	New

The size of the buffer used by pcap_next_packet in tsize, at line 397 of tcpdump/jni/libpcap/sf-pcap.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_next_packet passes to Address, at line 397 of tcpdump/jni/libpcap/sf-pcap.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap.c	tcpdump/jni/libpcap/sf-pcap.c
Line	412	513
Object	Address	tsize

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap.c
Method pcap_next_packet(pcap_t *p, struct pcap_pkthdr *hdr, u_char **data)

```
....
412.        amt_read = fread(&sf_hdr, 1, ps->hdrsize, fp);
....
513.                    tp = (u_char *)malloc(tsize);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=707
Status	New

The size of the buffer used by pcap_ng_check_header in bufsize, at line 645 of tcpdump/jni/libpcap/sf-pcap-ng.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pcap_ng_check_header passes to Address, at line 645 of tcpdump/jni/libpcap/sf-pcap-ng.c, to overwrite the target buffer.

	Source	Destination
File	tcpdump/jni/libpcap/sf-pcap-ng.c	tcpdump/jni/libpcap/sf-pcap-ng.c
Line	693	800
Object	Address	bufsize

Code Snippet
File Name tcpdump/jni/libpcap/sf-pcap-ng.c
Method pcap_ng_check_header(bpf_u_int32 magic, FILE *fp, u_int precision, char *errbuf,

```
....
693.        amt_read = fread(&total_length, 1, sizeof(total_length),
fp);
....
800.        p->buffer = malloc(p->bufsize);
```

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=1000001&projectid=2&pathid=967
Status	New

Method esp_print_decodesecret at line 515 of tcpdump/jni/tcpdump/print-esp.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	526	440
Object	ndo_espsecret	perror

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method void esp_print_decodesecret(netdissect_options *ndo)

```
....
526.        p = ndo->ndo_espsecret;
```

File Name tcpdump/jni/tcpdump/print-esp.c
Method static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
440.                    perror(filename);
```

Privacy Violation\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=968
Status	New

Method esp_print_decode_onesecret at line 406 of tcpdump/jni/tcpdump/print-esp.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	tcpdump/jni/tcpdump/print-esp.c	tcpdump/jni/tcpdump/print-esp.c
Line	438	440
Object	secretfile	perror

Code Snippet
File Name tcpdump/jni/tcpdump/print-esp.c
Method static void esp_print_decode_onesecret(netdissect_options *ndo, char *line,

```
....
438.                secretfile = fopen(filename, FOPEN_READ_TXT);
....
440.                        perror(filename);
```

Unsafe Use Of Target blank

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Unsafe Use Of Target blank Version:1

Categories

FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unsafe Use Of Target blank\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1550
Status	New

Using at line 208 of tcpdump/jni/libpcap/tests/visopts.py, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

	Source	Destination
File	tcpdump/jni/libpcap/tests/visopts.py	tcpdump/jni/libpcap/tests/visopts.py
Line	208	208
Object	<a id="lsvglink" target="_blank">	<a id="lsvglink" target="_blank">

Code Snippet
File Name tcpdump/jni/libpcap/tests/visopts.py
Method open this svg in browser

```
....
208.          <a id="lsvglink" target="_blank">open this svg in
browser</a>
```

Unsafe Use Of Target blank\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1551
Status	New

Using at line 213 of tcpdump/jni/libpcap/tests/visopts.py, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

	Source	Destination
File	tcpdump/jni/libpcap/tests/visopts.py	tcpdump/jni/libpcap/tests/visopts.py
Line	213	213
Object	<a id="rsvglink" target="_blank">	<a id="rsvglink" target="_blank">

Code Snippet
File Name tcpdump/jni/libpcap/tests/visopts.py
Method open this svg in browser

```
....
213.          <a id="rsvglink" target="_blank">open this svg in
browser</a>
```

Unsafe Use Of Target blank

Query Path:
Typescript\Cx\Typescript Low Visibility\Unsafe Use Of Target blank Version:1

Description

Unsafe Use Of Target blank\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1552
Status	New

Using at line 208 of tcpdump/jni/libpcap/tests/visopts.py, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

	Source	Destination
File	tcpdump/jni/libpcap/tests/visopts.py	tcpdump/jni/libpcap/tests/visopts.py
Line	208	208
Object	<a id="lsvglink" target="_blank">	<a id="lsvglink" target="_blank">

Code Snippet
File Name tcpdump/jni/libpcap/tests/visopts.py
Method open this svg in browser

```
....
208.          <a id="lsvglink" target="_blank">open this svg in
browser</a>
```

Unsafe Use Of Target blank\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=1553
Status	New

Using at line 213 of tcpdump/jni/libpcap/tests/visopts.py, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

	Source	Destination
File	tcpdump/jni/libpcap/tests/visopts.py	tcpdump/jni/libpcap/tests/visopts.py
Line	213	213
Object	<a id="rsvglink" target="_blank">	<a id="rsvglink" target="_blank">

Code Snippet
File Name tcpdump/jni/libpcap/tests/visopts.py
Method open this svg in browser

```
....
213.          <a id="rsvglink" target="_blank">open this svg in
browser</a>
```

Client Insufficient ClickJacking Protection

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Insufficient ClickJacking Protection Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)

Description

Client Insufficient ClickJacking Protection\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000001&projectid=2&pathid=705
Status	New

The application does not protect the web page tcpdump/jni/libpcap/doc/pcap.html from clickjacking attacks in legacy browsers, by using framebusting scripts.

	Source	Destination
File	tcpdump/jni/libpcap/doc/pcap.html	tcpdump/jni/libpcap/doc/pcap.html
Line	1	1
Object	CxJSNS_1933309730	CxJSNS_1933309730

Code Snippet

File Name	tcpdump/jni/libpcap/doc/pcap.html
Method	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">

```
....
1.  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```

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=1000001&projectid=2&pathid=713
Status	New

	Source	Destination
File	tcpdump/jni/libpcap/optimize.c	tcpdump/jni/libpcap/optimize.c
Line	202	202
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name tcpdump/jni/libpcap/optimize.c
Method find_levels_r(struct block *b)

```
....
202.              level = MAX(JT(b)->level, JF(b)->level) + 1;
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is

larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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 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

Off by One Error in Methods

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

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

Client Use Of JQuery Outdated Version

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)
        }

    }
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Short Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obselete since it is relatively easy to break. These obselete algorithms are vulnerable to several different kinds of attacks, including brute force.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.
- Do not use weak, outdated, or obsolete algorithms.
- Ensure you select the correct cryptographic mechanism according to the specific requirements.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
- Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
- Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
- For symmetric encryption, use a key length of at least 256 bits.

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.md5Hex(socialSecurityNum);
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.sha256Hex(socialSecurityNum);
}
```

Use of a One Way Hash without a Salt

Risk

What might happen

If an attacker gains access to the hashed passwords, she would likely be able to reverse the hash due to this weakness, and retrieve the original password. Once the passwords are discovered, the attacker can impersonate the users, and take full advantage of their privileges and access their personal data. Furthermore, this would likely not be discovered, as the attacker is being identified solely by the victims' credentials.

Cause

How does it happen

Typical cryptographic hashes, such as SHA-1 and MD5, are incredibly fast. Combined with attack techniques such as precomputed Rainbow Tables, it is relatively easy for attackers to reverse the hashes, and discover the original passwords. Lack of a unique, random salt added to the password makes brute force attacks even simpler.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.

- Do not use weak, outdated, or obsolete algorithms.

- Ensure you select the correct cryptographic mechanism according to the specific requirements.

Specific Recommendations:

- Passwords should be protected using a password hashing algorithm, instead of a general cryptographic hash. This includes adaptive hashes such as bcrypt, scrypt, PBKDF2 and Argon2.

- Tune the work factor, or cost, of the adaptive hash function according to the designated environment and risk profile.

- Do not use a regular cryptographic hash, such as SHA-1 or MD5, to protect passwords, as these are too fast.

- If it is necessary to use a common hash to protect passwords, add several bytes of unique, random data ("salt") to the password before hashing it. Store the salt with the hashed password, and do not reuse the same salt for multiple passwords.

Source Code Examples

Java

Unsalted Hashed Password

```
private String protectPassword(String password) {
```

```
      byte[] data = password.getBytes();
      byte[] hash = null;

      MessageDigest md = MessageDigest.getInstance("MD5");
      hash = md.digest(data);

      return Base64.getEncoder().encodeToString(hash);
}
```

Fast Hash with Salt

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
            MessageDigest md = MessageDigest.getInstance("SHA-1");

            SecureRandom rand = new SecureRandom();
            byte[] salt = new byte[32];
            rand.nextBytes(salt);

            md.update(salt);
            md.update(data);

            hash = md.digest();
    }
      catch (GeneralSecurityException gse) {
            handleCryptoErrors(gse);
    }
      finally {
            Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

Slow, Adaptive Password Hash

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
            SecureRandom rand = new SecureRandom();
            byte[] salt = new byte[32];
            rand.nextBytes(salt);

            SecretKeyFactory skf = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA512");
            PBEKeySpec spec = new PBEKeySpec(data, salt, ITERATION_COUNT, KEY_LENGTH);
            // ITERATION_COUNT should be configured by environment, KEY_LENGTH should be 256
            SecretKey key = skf.generateSecret(spec);

            hash = key.getEncoded();
    }
      catch (GeneralSecurityException gse) {
            handleCryptoErrors(gse);
    }
      finally {
            Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

Client Use Of JQuery Outdated Version

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

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Wrong Memory Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
```

```
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Potential 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
```

Client Insufficient ClickJacking Protection

Risk

What might happen

Clickjacking attacks allow an attacker to "hijack" a user's mouse clicks on a webpage, by invisibly framing the application, and superimposing it in front of a bogus site. When the user is convinced to click on the bogus website, e.g. on a link or a button, the user's mouse is actually clicking on the target webpage, despite being invisible.
This could allow the attacker to craft an overlay that, when clicked, would lead the user to perform undesirable actions in the vulnerable application, e.g. enabling the user's webcam, deleting all the user's records, changing the user's settings, or causing clickfraud.

Cause

How does it happen

The root cause of vulnerability to a clickjacking attack, is that the application's web pages can be loaded into a frame of another website. The application does not implement a proper frame-busting script, that would prevent the page from being loaded into another frame. Note that there are many types of simplistic redirection scripts that still leave the application vulnerable to clickjacking techniques, and should not be used.
When dealing with modern browsers, applications mitigate this vulnerability by issuing appropriate Content-Security-Policy or X-Frame-Options headers to indicate to the browser to disallow framing. However, many legacy browsers do not support this feature, and require a more manual approach by implementing a mitigation in Javascript. To ensure legacy support, a framebusting script is required.

General Recommendations

How to avoid it

Generic Guidance:

- Define and implement a a Content Security Policy (CSP) on the server side, including a frame-ancestors directive. Enforce the CSP on all relevant webpages.
- If certain webpages are required to be loaded into a frame, define a specific, whitelisted target URL.
- Alternatively, return a "X-Frame-Options" header on all HTTP responses. If it is necessary to allow a particular webpage to be loaded into a frame, define a specific, whitelisted target URL.
- For legacy support, implement framebusting code using Javascript and CSS to ensure that, if a page is framed, it is never displayed, and attempt to navigate into the frame to prevent attack. Even if navigation fails, the page is not displayed and is therefore not interactive, mitigating potential clickjacking attacks.

Specific Recommendations:

- Implement a proper framebuster script on the client, that is not vulnerable to frame-buster-busting attacks.
    - Code should first disable the UI, such that even if frame-busting is successfully evaded, the UI cannot be clicked. This can be done by setting the CSS value of the "display" attribute to "none" on either the "body" or "html" tags. This is done because, if a frame attempts to redirect and become the parent, the malicious parent can still prevent redirection via various techniques.
    - Code should then determine whether no framing occurs by comparing self === top; if the result is true, can the UI be enabled. If it is false, attempt to navigate away from the framing page by setting the top.location attribute to self.location.

Source Code Examples

JavaScript
Clickjackable Webpage

```
<html>
    <body>

     <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Bustable Framebuster

```
<html>
    <head>

     <script>
            if ( window.self.location != window.top.location ) {
                window.top.location = window.self.location;
            }
        </script>
    </head>

    <body>
        <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Proper Framebusterbusterbusting

```
<html>
    <head>

     <style> html {display : none; } </style>
        <script>
            if ( self === top ) {
                document.documentElement.style.display = 'block';
            }
            else {
                top.location = self.location;
            }
        </script>
    </head>

    <body>
        <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Heuristic 2nd Order Buffer Overflow malloc

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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 {
    //[..]
};
```

Potential Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
```

```
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

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 sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

Unsafe Use Of Target blank

Risk

What might happen

An unsuspecting user might click a vulnerable legitimate-looking link, prepared by an attacker, that leads to a malicious page. The new page that opens can redirect the **original** page to another malicious page and abuse the trust of the user to create a very convincing phishing attack.

Cause

How does it happen

When opening a new page using an <a> HTML element with the "target" attribute (with any value), or with window.open() within JavaScript, the new page has some access to the original page through the window.opener object. This may allow redirection to a malicious phishing page.

General Recommendations

How to avoid it

For HTML:

- Do not set the "target" attribute (with any value) for links created by users unless required.
- If required, when using the "target" attribute, also set the "rel" attribute as “noopener noreferrer”:
  - “noopener” for Chrome and Opera
  - “noreferrer” for Firefox and old browsers
  - No similar solution for Safari

For JavaScript:

- When invoking an untrusted new window using "var newWindow = window.open()", set "newWindow.opener=null" before setting "newWindow.location" to a potentially untrusted site, such that when the new site is open in the new window, it has no access to its original "opener" attribute

---

Source Code Examples

Unsafe Use Of Target blank

Risk

What might happen

An unsuspecting user might click a vulnerable legitimate-looking link, prepared by an attacker, that leads to a malicious page. The new page that opens can redirect the **original** page to another malicious page and abuse the trust of the user to create a very convincing phishing attack.

Cause

How does it happen

When opening a new page using an <a> HTML element with the "target" attribute (with any value), or with window.open() within JavaScript, the new page has some access to the original page through the window.opener object. This may allow redirection to a malicious phishing page.

General Recommendations

How to avoid it

For HTML:

- Do not set the "target" attribute (with any value) for links created by users unless required.
- If required, when using the "target" attribute, also set the "rel" attribute as “noopener noreferrer”:
  - “noopener” for Chrome and Opera
  - “noreferrer” for Firefox and old browsers
  - No similar solution for Safari

For JavaScript:

- When invoking an untrusted new window using "var newWindow = window.open()", set "newWindow.opener=null" before setting "newWindow.location" to a potentially untrusted site, such that when the new site is open in the new window, it has no access to its original "opener" attribute

---

Source Code Examples

JavaScript

Unsafe Use of Window.Open()

```
function newWindowOpener(untrustedURL) {
      var newWindow=window.open();
      newWindow.location=untrustedURL;
}
```

Safe Use of Window.Open()

```
function newWindowOpenerSafe(untrustedURL) {
      var newWindow=window.open();
      newWindow.opener=null;
      newWindow.location=untrustedURL;
}
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	6/19/2024
JavaScript	0831671993165974	6/19/2024
VbScript	1349101913133594	6/19/2024
Typescript	2047548555014888	6/19/2024
Common	0105849645654507	6/19/2024