src-1 Scan Report

Project Name	src-1
Scan Start	Saturday, June 22, 2024 1:11:04 AM
Preset	Checkmarx Default
Scan Time	00h:27m:55s
Lines Of Code Scanned	299746
Files Scanned	142
Report Creation Time	Saturday, June 22, 2024 1:41:45 AM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	7/1000 (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

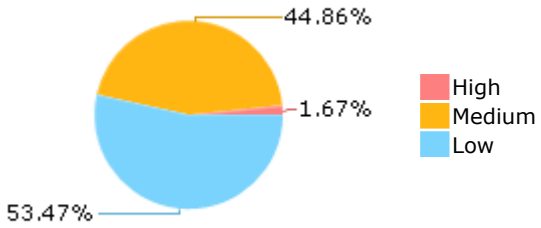
Results Limit

Results limit per query was set to 50

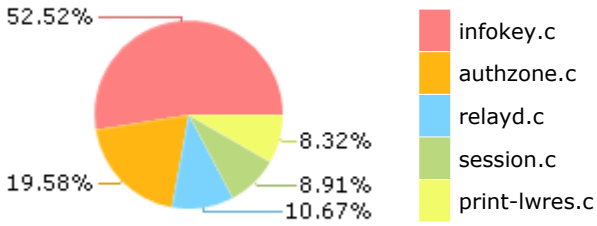
Selected Queries

Selected queries are listed in Result Summary

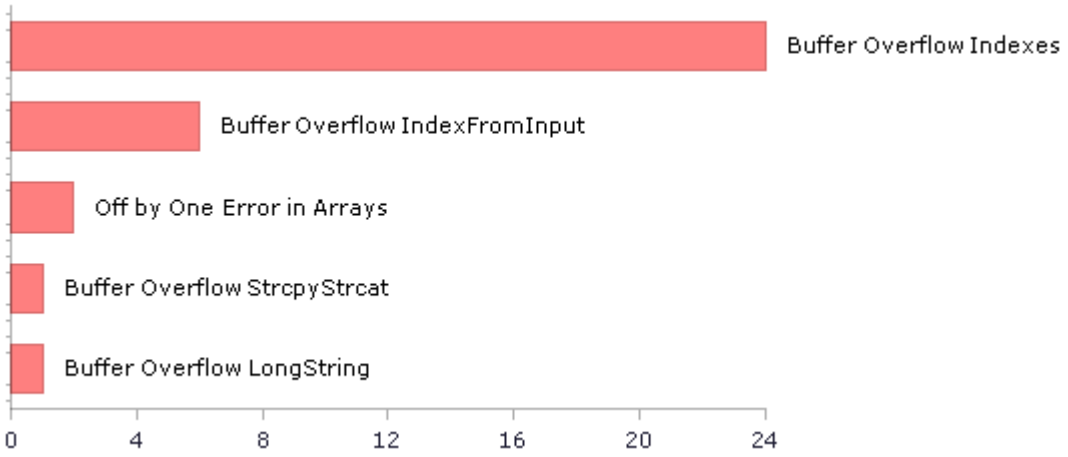
Result Summary



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	349	217
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	194	194
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	47	12
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	2	2
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	298	298
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	1	1
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	2	2
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	38	5
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	298	298
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	11	11
PCI DSS (3.2) - 6.5.2 - Buffer overflows	189	167
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.	25	25
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.	0	0
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.	25	23
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.	220	181
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.	2	2
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.	11	11

***** 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)	215	215
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)	4	2
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	14	8
SC-28 Protection of Information at Rest (P1)	1	1
SC-4 Information in Shared Resources (P1)	43	10
SC-5 Denial of Service Protection (P1)*	477	239
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	114	89
SI-11 Error Handling (P2)*	119	119
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	21	17

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

Scan Summary - OWASP Mobile Top 10 2016

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

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

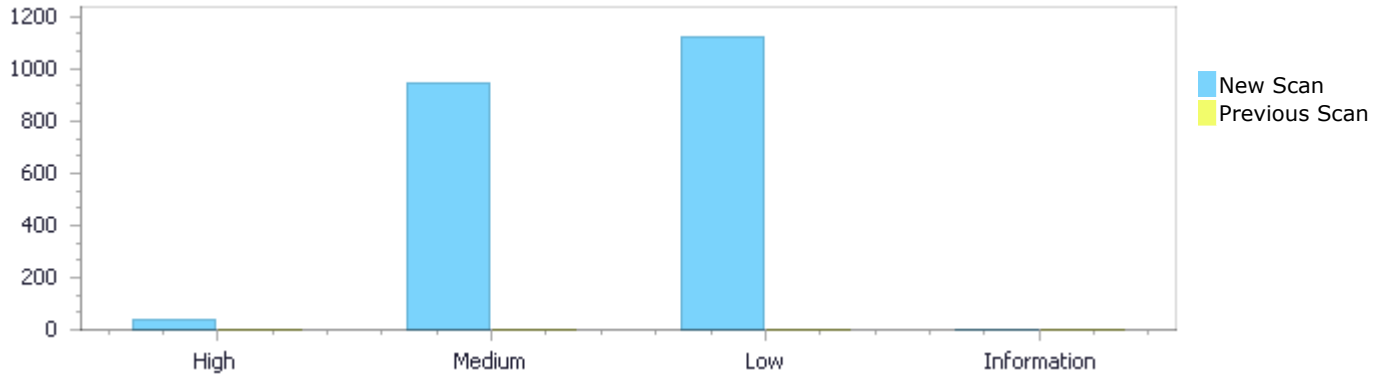
Scan Summary - Custom

Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	35	943	1,124	0	2,102
Recurrent Issues	0	0	0	0	0
Total	35	943	1,124	0	2,102
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	35	943	1,124	0	2,102
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	35	943	1,124	0	2,102

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow Indexes	24	High
Buffer Overflow IndexFromInput	6	High
Off by One Error in Arrays	2	High
Buffer Overflow LongString	1	High
Buffer Overflow StrcpyStrcat	1	High

Resource Injection	1	High
Dangerous Functions	284	Medium
MemoryFree on StackVariable	132	Medium
Buffer Overflow boundcpy WrongSizeParam	124	Medium
Use of Zero Initialized Pointer	121	Medium
Memory Leak	86	Medium
Use of Uninitialized Pointer	84	Medium
Wrong Size t Allocation	36	Medium
Use of Uninitialized Variable	17	Medium
Char Overflow	14	Medium
Buffer Overflow AddressOfLocalVarReturned	10	Medium
Double Free	9	Medium
Integer Overflow	7	Medium
Stored Buffer Overflow boundcpy	6	Medium
Inadequate Encryption Strength	4	Medium
Boolean Overflow	3	Medium
Divide By Zero	3	Medium
Heap Inspection	2	Medium
Wrong Memory Allocation	1	Medium
Sizeof Pointer Argument	435	Low
Improper Resource Access Authorization	169	Low
NULL Pointer Dereference	159	Low
Unchecked Return Value	119	Low
Unchecked Array Index	51	Low
Privacy Violation	36	Low
TOCTOU	28	Low
Incorrect Permission Assignment For Critical Resources	25	Low
Use of Sizeof On a Pointer Type	24	Low
Exposure of System Data to Unauthorized Control Sphere	21	Low
Reliance on DNS Lookups in a Decision	14	Low
Use of Obsolete Functions	14	Low
Potential Off by One Error in Loops	10	Low
Inconsistent Implementations	6	Low
Insecure Temporary File	5	Low
Heuristic 2nd Order Buffer Overflow read	3	Low
Potential Path Traversal	2	Low
Potential Precision Problem	2	Low
Information Exposure Through Comments	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
src-1/authzone.c	121
src-1/relayd.c	64
src-1/lex.c	56
src-1/cd.c	36
src-1/pf.c	36
src-1/replay.c	35
src-1/channels.c	31

src-1/cachedump.c	30
src-1/server.c	29
src-1/servconf.c	27

Scan Results Details

Buffer Overflow Indexes

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

Categories

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

Description

Buffer Overflow Indexes\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_getc_ passes to getc, at line 534 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	539	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_getc_ (FILE *finput)

```
....
539.      return getc (finput);
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=3
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_getc_ passes to getc, at line 534 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	546	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_getc_ (FILE *finput)

```
....
546.    return getc (finput);
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=4
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	552	763
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
552.    register int c = getc (finput);
```

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
763.                p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=5
Status	New

The size of the buffer used by ffelex_cfelex_ in buffer_length, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	552	764
Object	getc	buffer_length

Code Snippet

File Name	src-1/lex.c
Method	ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
552.    register int c = getc (finput);
```

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
764.                r = &q[buffer_length];
```

Buffer Overflow Indexes\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=6
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination

File	src-1/lex.c	src-1/lex.c
Line	552	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
552.    register int c = getc (finput);
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=7
Status New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	568	763
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
568.          c = getc (finput);
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
763.                p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=8
Status	New

The size of the buffer used by ffelex_cfelex_ in buffer_length, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	568	764
Object	getc	buffer_length

Code Snippet

File Name src-1/lex.c

Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
568.          c = getc (finput);
```

File Name src-1/lex.c

Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
764.                r = &q[buffer_length];
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=9
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	568	703
Object	getc	bytes_used

Code Snippet

File Name src-1/lex.c
Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
568.          c = getc (finput);
```

File Name src-1/lex.c

Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=10
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	605	763
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
605.          c = getc (finput);
```

File Name src-1/lex.c

Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
763.                p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=11

Status	New

The size of the buffer used by ffelex_cfelex_ in buffer_length, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	605	764
Object	getc	buffer_length

Code Snippet
File Name src-1/lex.c
Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
605.          c = getc (finput);
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
764.                r = &q[buffer_length];
```

Buffer Overflow Indexes\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=12
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfebackslash_ passes to getc, at line 550 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	605	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_cfebackslash_ (int *use_d, int *d, FILE *finput)

```
....
605.          c = getc (finput);
```

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=13
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfelex_ passes to getc, at line 674 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	734	763
Object	getc	bytes_used

Code Snippet

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
734.              c = getc (finput);
....
763.                p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=14
Status	New

The size of the buffer used by ffelex_cfelex_ in buffer_length, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfelex_ passes to getc, at line 674 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	734	764
Object	getc	buffer_length

Code Snippet

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
734.              c = getc (finput);
....
764.                r = &q[buffer_length];
```

Buffer Overflow Indexes\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=15
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_cfelex_ passes to getc, at line 674 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	770	703
Object	getc	bytes_used

Code Snippet

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
770.            c = getc (finput);
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=16
Status	New

The size of the buffer used by ffelex_get_directive_line_ in bytes_used, at line 920 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_get_directive_line_ passes to getc, at line 920 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	953	949
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_get_directive_line_ (char **text, FILE *finput)

```
....
953.         c = getc (finput);
....
949.           p = &directive_buffer[bytes_used];
```

Buffer Overflow Indexes\Path 16:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=17
Status New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1041	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_hash_ (FILE *finput)

```
....
1041.              && ((c = getc (finput)) == ' ' || c == '\t' || c ==
'\n'
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.               p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 17:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=18
Status New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1091	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_hash_ (FILE *finput)

```
....
1091.             && ((c = getc (finput)) == ' ' || c == '\t' || c ==
'\n'
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=19
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1110	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_hash_ (FILE *finput)

```
....
1110.             && ((c = getc (finput)) == ' ' || c == '\t' || c ==
'\n'
```

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=20
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1128	703
Object	getc	bytes_used

Code Snippet

File Name	src-1/lex.c
Method	ffelex_hash_ (FILE *finput)

```
....
1128.             && ((c = getc (finput)) == ' ' || c == '\t'))
```

File Name	src-1/lex.c
Method	ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=21
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination

File	src-1/lex.c	src-1/lex.c
Line	1137	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_hash_ (FILE *finput)

```
....
1137.             && ((c = getc (finput)) == ' ' || c == '\t'))
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 21:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=22
Status New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1145	703
Object	getc	bytes_used

Code Snippet
File Name src-1/lex.c
Method ffelex_hash_ (FILE *finput)

```
....
1145.             c = getc (finput);
```

File Name src-1/lex.c
Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=23
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1256	703
Object	getc	bytes_used

Code Snippet

File Name src-1/lex.c

Method ffelex_hash_ (FILE *finput)

```
....
1256.       c = getc (finput);
```

File Name src-1/lex.c

Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=24
Status	New

The size of the buffer used by ffelex_cfelex_ in bytes_used, at line 674 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_hash_ passes to getc, at line 1017 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1301	703
Object	getc	bytes_used

Code Snippet

File Name src-1/lex.c
Method ffelex_hash_ (FILE *finput)

```
....
1301.           c = getc (finput);
```

File Name src-1/lex.c

Method ffelex_cfelex_ (ffelexToken *xtoken, FILE *finput, int c)

```
....
703.              p = &q[bytes_used];
```

Buffer Overflow Indexes\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=25
Status	New

The size of the buffer used by main in strcspn, at line 342 of src-1/tmux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to getenv, at line 342 of src-1/tmux.c, to overwrite the target buffer.

	Source	Destination
File	src-1/tmux.c	src-1/tmux.c
Line	509	512
Object	getenv	strcspn

Code Snippet
File Name src-1/tmux.c
Method main(int argc, char **argv)

```
....
509.              s = getenv("TMUX");
....
512.                    path[strcspn(path, ",")] = '\0';
```

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=1050100&projectid=50090&pathid=26
Status	New

The size of the buffer used by ffelex_file_fixed in c, at line 1764 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_getc_ passes to getc, at line 534 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	539	1848
Object	getc	c

Code Snippet
File Name src-1/lex.c
Method ffelex_getc_ (FILE *finput)

```
....
539.      return getc (finput);
```

File Name src-1/lex.c
Method ffelex_file_fixed (ffewhereFile wf, FILE *f)

```
....
1848.    while (((lextype = ffelex_first_char_[c]) ==
FFELEX_typeCOMMENT)
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=27
Status	New

The size of the buffer used by ffelex_file_fixed in c, at line 1764 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_getc_ passes to getc, at line 534 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	546	1848
Object	getc	c

Code Snippet
File Name src-1/lex.c
Method ffelex_getc_ (FILE *finput)

```
....
546.    return getc (finput);
```

File Name src-1/lex.c

Method ffelex_file_fixed (ffewhereFile wf, FILE *f)

```
....
1848.    while (((lextype = ffelex_first_char_[c]) ==
FFELEX_typeCOMMENT)
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=28
Status	New

The size of the buffer used by ffelex_file_fixed in c, at line 1764 of src-1/lex.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ffelex_file_fixed passes to getc, at line 1764 of src-1/lex.c, to overwrite the target buffer.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1899	1848
Object	getc	c

Code Snippet

File Name src-1/lex.c

Method ffelex_file_fixed (ffewhereFile wf, FILE *f)

```
....
1899.        c = getc (f);
....
1848.    while (((lextype = ffelex_first_char_[c]) ==
FFELEX_typeCOMMENT)
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=29
Status	New

The size of the buffer used by main in strcspn, at line 342 of src-1/tmux.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to getenv, at line 342 of src-1/tmux.c, to overwrite the target buffer.

	Source	Destination

File	src-1/tmux.c	src-1/tmux.c
Line	509	512
Object	getenv	strcspn

Code Snippet
File Name src-1/tmux.c
Method main(int argc, char **argv)

```
....
509.                s = getenv("TMUX");
....
512.                      path[strcspn(path, ",")] = '\0';
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=30
Status	New

The size of the buffer used by rule_add in strcspn, at line 885 of src-1/relayd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rule_add passes to buf, at line 885 of src-1/relayd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	935	937
Object	buf	strcspn

Code Snippet
File Name src-1/relayd.c
Method rule_add(struct protocol *proto, struct relay_rule *rule, const char *rulefile)

```
....
935.        while (fgets(buf, sizeof(buf), fp) != NULL) {
....
937.              buf[strcspn(buf, "\r\n\t ")] = '\0';
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=31
Status	New

The size of the buffer used by recvlink in i, at line 1103 of src-1/server.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that recvlink passes to tbuf, at line 1103 of src-1/server.c, to overwrite the target buffer.

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	1128	1129
Object	tbuf	i

Code Snippet
File Name src-1/server.c
Method recvlink(char *new, opt_t opts, int mode, off_t size)

```
....
1128.       if ((i = readlink(target, tbuf, sizeof(tbuf)-1)) != -1) {
1129.             tbuf[i] = '\0';
```

Off by One Error in Arrays

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Off by One Error in Arrays\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=32
Status	New

The buffer allocated by sizeof in src-1/respip.c at line 567 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	579	579
Object	sizeof	sizeof

Code Snippet
File Name src-1/respip.c
Method rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i,

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

Off by One Error in Arrays\Path 2:

Severity	High
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=33
Status	New

The buffer allocated by sizeof in src-1/respip.c at line 567 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	588	588
Object	sizeof	sizeof

Code Snippet
File Name src-1/respip.c
Method rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i,

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

Buffer Overflow LongString

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

Categories

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

Description
Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1
Status	New

The size of the buffer used by sys___tmpfd in path, at line 1210 of src-1/vfs_syscalls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sys___tmpfd passes to "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789_-", at line 1210 of src-1/vfs_syscalls.c, to overwrite the target buffer.

	Source	Destination
File	src-1/vfs_syscalls.c	src-1/vfs_syscalls.c
Line	1224	1243
Object	"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789_-"	path

Code Snippet

File Name	src-1/vfs_syscalls.c
Method	sys___tmpfd(struct proc *p, void *v, register_t *retval)

```
....
1224.       static const char *letters =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789_-";
....
1243.             path[i] = letters[(unsigned char)path[i] & 63];
```

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=1050100&projectid=50090&pathid=34
Status	New

The size of the buffer used by common_handle_option in arg, at line 674 of src-1/opts.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that common_handle_option passes to arg, at line 674 of src-1/opts.c, to overwrite the target buffer.

	Source	Destination
File	src-1/opts.c	src-1/opts.c
Line	674	721
Object	arg	arg

Code Snippet

File Name	src-1/opts.c
Method	common_handle_option (size_t scode, const char *arg, int value,

```
....
674.  common_handle_option (size_t scode, const char *arg, int value,
....
721.        strcpy (new_option+1, arg);
```

Resource Injection

Query Path:
CPP\Cx\CPP High Risk\Resource Injection Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Resource Injection\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=340
Status	New

The application's connect_local_xsocket method, at line 4980 of src-1/channels.c, opens a network socket. The application connects the socket to an address, connect. This endpoint is defined using untrusted data.
This may enable an attacker to control the application's socket address, leading to a Resource Injection attack.

An attacker may be able to control the remote address or port for the socket, by altering the user input getenv, in method x11_connect_display of src-1/channels.c, line 4999. This value is then used directly to open and connect the socket to the remote server.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	5009	4991
Object	getenv	connect

Code Snippet
File Name src-1/channels.c
Method x11_connect_display(struct ssh *ssh)

```
....
5009.       display = getenv("DISPLAY");
```

File Name src-1/channels.c
Method connect_local_xsocket(u_int dnr)

```
....
4991.       if (connect(sock, (struct sockaddr *)&addr, sizeof(addr)) ==
0)
```

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=1050100&projectid=50090&pathid=365
Status	New

The dangerous function, memcpy, was found in use at line 128 in src-1/amdgpu_dm_plane.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/amdgpu_dm_plane.c	src-1/amdgpu_dm_plane.c
Line	143	143
Object	memcpy	memcpy

Code Snippet
File Name src-1/amdgpu_dm_plane.c
Method static void add_modifier(uint64_t **mods, uint64_t *size, uint64_t *cap, uint64_t mod)

```
....
143.              memcpy(new_mods, *mods, sizeof(uint64_t) * *size);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=366
Status	New

The dangerous function, memcpy, was found in use at line 795 in src-1/authzone.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	809	809
Object	memcpy	memcpy

Code Snippet
File Name src-1/authzone.c
Method rrset_add_rr(struct auth_rrset* rrset, uint32_t rr_ttl, uint8_t* rdata,

```
....
809.         memcpy(d, old, sizeof(struct packed_rrset_data));
```

Dangerous Functions\Path 3:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=367
Status	New

The dangerous function, memcpy, was found in use at line 936 in src-1/authzone.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	963	963
Object	memcpy	memcpy

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
963.        memcpy(d, old, sizeof(struct packed_rrset_data));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=368
Status	New

The dangerous function, memcpy, was found in use at line 936 in src-1/authzone.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1027	1027
Object	memcpy	memcpy

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
1027.       memcpy(sigd, sigold, sizeof(struct packed_rrset_data));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=369
Status	New

The dangerous function, memcpy, was found in use at line 1567 in src-1/authzone.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1613	1613
Object	memcpy	memcpy

Code Snippet
File Name src-1/authzone.c
Method auth_zone_read_zonefile(struct auth_zone* z, struct config_file* cfg)

```
....
1613.             memcpy(state.origin, z->name, z->namelen);
```

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=370
Status New

The dangerous function, memcpy, was found in use at line 2632 in src-1/authzone.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	2642	2642
Object	memcpy	memcpy

Code Snippet
File Name src-1/authzone.c
Method synth_cname_buf(uint8_t* qname, size_t qname_len, size_t dname_len,

```
....
2642.       memcpy(buf, qname, qname_len-dname_len);
```

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=371
Status New

The dangerous function, memcpy, was found in use at line 98 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	171	171
Object	memcpy	memcpy

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
171.        memcpy(&(pdu->ap_header), &header, sizeof(header));
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=372
Status	New

The dangerous function, memcpy, was found in use at line 1218 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1227	1227
Object	memcpy	memcpy

Code Snippet
File Name src-1/ax.c
Method ax_pdu_add_uint16(struct ax *ax, uint16_t value)

```
....
1227.       memcpy(ax->ax_wbuf + ax->ax_wbtlen, &value, sizeof(value));
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=373
Status	New

The dangerous function, memcpy, was found in use at line 1233 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c

Line	1242	1242
Object	memcpy	memcpy

Code Snippet
File Name src-1/ax.c
Method ax_pdu_add_uint32(struct ax *ax, uint32_t value)

```
....
1242.       memcpy(ax->ax_wbuf + ax->ax_wbtlen, &value, sizeof(value));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=374
Status	New

The dangerous function, memcpy, was found in use at line 1248 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1257	1257
Object	memcpy	memcpy

Code Snippet
File Name src-1/ax.c
Method ax_pdu_add_uint64(struct ax *ax, uint64_t value)

```
....
1257.       memcpy(ax->ax_wbuf + ax->ax_wbtlen, &value, sizeof(value));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=375
Status	New

The dangerous function, memcpy, was found in use at line 1298 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1311	1311
Object	memcpy	memcpy

Code Snippet
File Name src-1/ax.c
Method ax_pdu_add_str(struct ax *ax, struct ax_ostring *str)

```
....
1311.       memcpy(&(ax->ax_wbuf[ax->ax_wbtlen]), str->aos_string, str-
>aos_slen);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=376
Status	New

The dangerous function, memcpy, was found in use at line 1387 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1391	1391
Object	memcpy	memcpy

Code Snippet
File Name src-1/ax.c
Method ax_pdutoh16(struct ax_pdu_header *header, uint8_t *buf)

```
....
1391.       memcpy(&value, buf, sizeof(value));
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=377
Status	New

The dangerous function, memcpy, was found in use at line 1398 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1402	1402
Object	memcpy	memcpy

Code Snippet

File Name	src-1/ax.c
Method	ax_pdutoh32(struct ax_pdu_header *header, uint8_t *buf)

```
....
1402.       memcpy(&value, buf, sizeof(value));
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=378
Status	New

The dangerous function, memcpy, was found in use at line 1409 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1413	1413
Object	memcpy	memcpy

Code Snippet	
File Name	src-1/ax.c
Method	ax_pdutoh64(struct ax_pdu_header *header, uint8_t *buf)

```
....
1413.       memcpy(&value, buf, sizeof(value));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=379
Status	New

The dangerous function, memcpy, was found in use at line 1456 in src-1/ax.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1471	1471
Object	memcpy	memcpy

Code Snippet	
File Name	src-1/ax.c
Method	ax_pdutoostring(struct ax_pdu_header *header,

```
....
1471.       memcpy(ostring->aos_string, buf, ostring->aos_slen);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=380
Status	New

The dangerous function, memcpy, was found in use at line 720 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	782	782
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method cdioctl(dev_t dev, u_long cmd, caddr_t addr, int flag, struct proc *p)

```
....
782.              memcpy(sc->sc_dk.dk_label, lp, sizeof(*lp));
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=381
Status	New

The dangerous function, memcpy, was found in use at line 720 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	881	881
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method cdioctl(dev_t dev, u_long cmd, caddr_t addr, int flag, struct proc *p)

```
....
881.                    memcpy(addr, th, sizeof(*th));
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=382
Status	New

The dangerous function, memcpy, was found in use at line 1638 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1685	1685
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_auth(struct cd_softc *sc, union dvd_authinfo *a)

```
....
1685.                    dvd_copy_challenge(a->lsc.chal, &buf[4]);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=383
Status	New

The dangerous function, memcpy, was found in use at line 1638 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1699	1699
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_auth(struct cd_softc *sc, union dvd_authinfo *a)

```
....
1699.                   dvd_copy_key(a->lsk.key, &buf[4]);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=384
Status	New

The dangerous function, memcpy, was found in use at line 1638 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1717	1717
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_auth(struct cd_softc *sc, union dvd_authinfo *a)

```
....
1717.                   dvd_copy_key(a->lstk.title_key, &buf[5]);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=385
Status	New

The dangerous function, memcpy, was found in use at line 1638 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1740	1740
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_auth(struct cd_softc *sc, union dvd_authinfo *a)

```
....
1740.             dvd_copy_challenge(&buf[4], a->hsc.chal);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=386
Status	New

The dangerous function, memcpy, was found in use at line 1638 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1756	1756
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_auth(struct cd_softc *sc, union dvd_authinfo *a)

```
....
1756.             dvd_copy_key(&buf[4], a->hsk.key);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=387
Status	New

The dangerous function, memcpy, was found in use at line 1921 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1952	1952
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_read_disckey(struct cd_softc *sc, union dvd_struct *s)

```
....
1952.             memcpy(s->diskey.value, buf->data, sizeof(s-
>diskey.value));
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=388
Status	New

The dangerous function, memcpy, was found in use at line 1961 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1994	1994
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_read_bca(struct cd_softc *sc, union dvd_struct *s)

```
....
1994.             memcpy(s->bca.value, &buf[4], s->bca.len);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=389
Status	New

The dangerous function, memcpy, was found in use at line 2002 in src-1/cd.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	2034	2034
Object	memcpy	memcpy

Code Snippet
File Name src-1/cd.c
Method dvd_read_manufact(struct cd_softc *sc, union dvd_struct *s)

```
....
2034.                    memcpy(s->manufact.value, buf->data, s-
>manufact.len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=390
Status	New

The dangerous function, memcpy, was found in use at line 1241 in src-1/channels.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	1302	1302
Object	memcpy	memcpy

Code Snippet
File Name src-1/channels.c
Method x11_open_helper(struct ssh *ssh, struct sshbuf *b)

```
....
1302.        memcpy(ucp + 12 + ((proto_len + 3) & ~3),
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=391
Status	New

The dangerous function, memcpy, was found in use at line 1497 in src-1/channels.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	1549	1549
Object	memcpy	memcpy

Code Snippet
File Name src-1/channels.c
Method channel_decode_socks5(Channel *c, struct sshbuf *input, struct sshbuf *output)

```
....
1549.       memcpy(&s5_req, p, sizeof(s5_req));
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=392
Status	New

The dangerous function, memcpy, was found in use at line 208 in src-1/cms_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/cms_enc.c	src-1/cms_enc.c
Line	217	217
Object	memcpy	memcpy

Code Snippet
File Name src-1/cms_enc.c
Method cms_EncryptedContent_init(CMS_EncryptedContentInfo *ec,

```
....
217.              memcpy(ec->key, key, keylen);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=393
Status	New

The dangerous function, memcpy, was found in use at line 484 in src-1/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	516	516
Object	memcpy	memcpy

Code Snippet
File Name src-1/d1_both.c
Method dtls1_retrieve_buffered_fragment(SSL *s, long max, int *ok)

```
....
516.                    memcpy(&p[frag->msg_header.frag_off],
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=394
Status	New

The dangerous function, memcpy, was found in use at line 553 in src-1/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	580	580
Object	memcpy	memcpy

Code Snippet
File Name src-1/d1_both.c
Method dtls1_reassemble_fragment(SSL *s, struct hm_header_st* msg_hdr, int *ok)

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

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=395
Status	New

The dangerous function, memcpy, was found in use at line 653 in src-1/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	708	708
Object	memcpy	memcpy

Code Snippet
File Name src-1/d1_both.c
Method dtls1_process_out_of_seq_message(SSL *s, struct hm_header_st* msg_hdr, int *ok)

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

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=396
Status	New

The dangerous function, memcpy, was found in use at line 939 in src-1/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	957	957
Object	memcpy	memcpy

Code Snippet
File Name src-1/d1_both.c
Method dtls1_buffer_message(SSL *s, int is_ccs)

```
....
957.        memcpy(frag->fragment, s->init_buf->data, s->init_num);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=397
Status	New

The dangerous function, memcpy, was found in use at line 992 in src-1/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	1030	1030
Object	memcpy	memcpy

Code Snippet
File Name src-1/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
....
1030.       memcpy(s->init_buf->data, frag->fragment,
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=398
Status	New

The dangerous function, memcpy, was found in use at line 122 in src-1/dt_prov_syscall.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/dt_prov_syscall.c	src-1/dt_prov_syscall.c
Line	156	156
Object	memcpy	memcpy

Code Snippet
File Name src-1/dt_prov_syscall.c
Method dt_prov_syscall_entry(struct dt_provider *dtpv, ...)

```
....
156.                    memcpy(dtev->dtev_args, args, argsize);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=399
Status	New

The dangerous function, memcpy, was found in use at line 113 in src-1/e_rc4_hmac_md5.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/e_rc4_hmac_md5.c	src-1/e_rc4_hmac_md5.c
Line	160	160
Object	memcpy	memcpy

Code Snippet
File Name src-1/e_rc4_hmac_md5.c
Method rc4_hmac_md5_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
160.                            memcpy(out + rc4_off, in + rc4_off,
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=400
Status	New

The dangerous function, memcpy, was found in use at line 229 in src-1/e_rc4_hmac_md5.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/e_rc4_hmac_md5.c	src-1/e_rc4_hmac_md5.c
Line	246	246
Object	memcpy	memcpy

Code Snippet
File Name src-1/e_rc4_hmac_md5.c
Method rc4_hmac_md5_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg, void *ptr)

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

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=401
Status	New

The dangerous function, memcpy, was found in use at line 486 in src-1/ExternalFunctions.cpp file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	488	488
Object	memcpy	memcpy

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_memcpy(FunctionType *FT,

```
....
488.    memcpy(GVTOP(Args[0]), GVTOP(Args[1]),
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=402
Status	New

The dangerous function, memcpy, was found in use at line 337 in src-1/ExternalFunctions.cpp file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	375	375
Object	memcpy	memcpy

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
375.          memcpy(Buffer, "%", 2); break;
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=403
Status	New

The dangerous function, memcpy, was found in use at line 337 in src-1/ExternalFunctions.cpp file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	408	408
Object	memcpy	memcpy

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
408.        memcpy(OutputBuffer, Buffer, Len + 1);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=404
Status	New

The dangerous function, memcpy, was found in use at line 786 in src-1/glob.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/glob.c	src-1/glob.c
Line	850	850
Object	memcpy	memcpy

Code Snippet
File Name src-1/glob.c
Method globextend(const Char *path, glob_t *pglob, struct glob_lim *limitp,

```
....
850.                    memcpy(statv[pglob->gl_offs + pglob->gl_pathc],
sb,
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=405
Status	New

The dangerous function, memcpy, was found in use at line 161 in src-1/i915_gpu_error.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	173	173
Object	memcpy	memcpy

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void i915_error_puts(struct drm_i915_error_state_buf *e, const char *str)

```
....
173.        memcpy(e->buf + e->bytes, str, len);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=406
Status	New

The dangerous function, memcpy, was found in use at line 972 in src-1/i915_gpu_error.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1023	1023
Object	memcpy	memcpy

Code Snippet
File Name src-1/i915_gpu_error.c
Method ssize_t i915_gpu_coredump_copy_to_buffer(struct i915_gpu_coredump *error,

```
....
1023.             memcpy(buf, page_address(sg_page(sg)) + start, len);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=407
Status	New

The dangerous function, memcpy, was found in use at line 1727 in src-1/i915_gpu_error.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1737	1737
Object	memcpy	memcpy

Code Snippet
File Name src-1/i915_gpu_error.c
Method gt_record_uc(struct intel_gt_coredump *gt,

```
....
1737.       memcpy(&error_uc->guc_fw, &uc->guc.fw, sizeof(uc->guc.fw));
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=408
Status	New

The dangerous function, memcpy, was found in use at line 1727 in src-1/i915_gpu_error.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1738	1738
Object	memcpy	memcpy

Code Snippet
File Name src-1/i915_gpu_error.c
Method gt_record_uc(struct intel_gt_coredump *gt,

```
....
1738.       memcpy(&error_uc->huc_fw, &uc->huc.fw, sizeof(uc->huc.fw));
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=409
Status	New

The dangerous function, memcpy, was found in use at line 1913 in src-1/i915_gpu_error.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1915	1915
Object	memcpy	memcpy

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void gt_record_info(struct intel_gt_coredump *gt)

```
....
1915.       memcpy(&gt->info, &gt->_gt->info, sizeof(struct
intel_gt_info));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=410
Status	New

The dangerous function, memcpy, was found in use at line 1975 in src-1/i915_gpu_error.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1987	1987
Object	memcpy	memcpy

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void capture_gen(struct i915_gpu_coredump *error)

```
....
1987.       memcpy(&error->device_info,
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=411
Status	New

The dangerous function, memcpy, was found in use at line 1975 in src-1/i915_gpu_error.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1990	1990
Object	memcpy	memcpy

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void capture_gen(struct i915_gpu_coredump *error)

```
....
1990.       memcpy(&error->runtime_info,
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=412
Status	New

The dangerous function, memcpy, was found in use at line 839 in src-1/ip6_input.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	875	875
Object	memcpy	memcpy

Code Snippet
File Name src-1/ip6_input.c
Method ip6_process_hopopts(struct mbuf **mp, u_int8_t *opthead, int hbhlen,

```
....
875.                    memcpy((caddr_t)&rtalert_val, (caddr_t)(opt +
2), 2);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=413
Status	New

The dangerous function, memcpy, was found in use at line 839 in src-1/ip6_input.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	910	910
Object	memcpy	memcpy

Code Snippet
File Name src-1/ip6_input.c
Method ip6_process_hopopts(struct mbuf **mp, u_int8_t *opthead, int hbhlen,

```
....
910.                    memcpy(&jumboplen, opt + 2, sizeof(jumboplen));
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=414
Status	New

The dangerous function, memcpy, was found in use at line 1015 in src-1/ip6_input.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	1032	1032
Object	memcpy	memcpy

Code Snippet
File Name src-1/ip6_input.c
Method ip6_savecontrol(struct inpcb *in6p, struct mbuf *m, struct mbuf **mp)

```
....
1032.              memcpy(&pi6.ipi6_addr, &ip6->ip6_dst, sizeof(struct
in6_addr));
```

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=1050100&projectid=50090&pathid=172
Status	New

Calling free() (line 123) on a variable that was not dynamically allocated (line 123) in file src-1/asn1_item.c may result with a crash.

	Source	Destination
File	src-1/asn1_item.c	src-1/asn1_item.c
Line	134	134
Object	str	str

Code Snippet

File Name	src-1/asn1_item.c
Method	ASN1_item_digest(const ASN1_ITEM *it, const EVP_MD *type, void *asn,

```
....
134.                free(str);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=173
Status	New

Calling free() (line 123) on a variable that was not dynamically allocated (line 123) in file src-1/asn1_item.c may result with a crash.

	Source	Destination
File	src-1/asn1_item.c	src-1/asn1_item.c
Line	138	138
Object	str	str

Code Snippet	
File Name	src-1/asn1_item.c
Method	ASN1_item_digest(const ASN1_ITEM *it, const EVP_MD *type, void *asn,

```
....
138.        free(str);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=174
Status	New

Calling free() (line 149) on a variable that was not dynamically allocated (line 149) in file src-1/asn1_item.c may result with a crash.

	Source	Destination
File	src-1/asn1_item.c	src-1/asn1_item.c
Line	166	166
Object	b	b

Code Snippet	
File Name	src-1/asn1_item.c
Method	ASN1_item_dup(const ASN1_ITEM *it, void *x)

```
....
166.        free(b);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=175
Status	New

Calling free() (line 612) on a variable that was not dynamically allocated (line 612) in file src-1/asn1_item.c may result with a crash.

	Source	Destination
File	src-1/asn1_item.c	src-1/asn1_item.c
Line	634	634
Object	b	b

Code Snippet
File Name src-1/asn1_item.c
Method ASN1_item_i2d_bio(const ASN1_ITEM *it, BIO *out, void *x)

```
....
634.        free(b);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=176
Status	New

Calling free() (line 795) on a variable that was not dynamically allocated (line 795) in file src-1/authzone.c may result with a crash.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	859	859
Object	old	old

Code Snippet
File Name src-1/authzone.c
Method rrset_add_rr(struct auth_rrset* rrset, uint32_t rr_ttl, uint8_t* rdata,

```
....
859.        free(old);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=177
Status	New

Calling free() (line 1567) on a variable that was not dynamically allocated (line 1567) in file src-1/authzone.c may result with a crash.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1592	1592
Object	n	n

Code Snippet
File Name src-1/authzone.c
Method auth_zone_read_zonefile(struct auth_zone* z, struct config_file* cfg)

```
....
1592.                    free(n);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=178
Status	New

Calling free() (line 1567) on a variable that was not dynamically allocated (line 1567) in file src-1/authzone.c may result with a crash.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1597	1597
Object	n	n

Code Snippet
File Name src-1/authzone.c
Method auth_zone_read_zonefile(struct auth_zone* z, struct config_file* cfg)

```
....
1597.               free(n);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=179
Status	New

Calling free() (line 1567) on a variable that was not dynamically allocated (line 1567) in file src-1/authzone.c may result with a crash.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1621	1621
Object	n	n

Code Snippet
File Name src-1/authzone.c
Method auth_zone_read_zonefile(struct auth_zone* z, struct config_file* cfg)

```
....
1621.               free(n);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=180
Status	New

Calling free() (line 2267) on a variable that was not dynamically allocated (line 2267) in file src-1/authzone.c may result with a crash.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	2275	2275
Object	c	c

Code Snippet
File Name src-1/authzone.c
Method auth_chunks_delete(struct auth_transfer* at)

```
....
2275.                   free(c);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=181
Status	New

Calling free() (line 316) on a variable that was not dynamically allocated (line 316) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	347	347
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_basic(void)

```
....
347.        free(buf);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=182
Status	New

Calling free() (line 352) on a variable that was not dynamically allocated (line 352) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	386	386
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_add_space(void)

```
....
386.        free(buf);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=183
Status	New

Calling free() (line 420) on a variable that was not dynamically allocated (line 420) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	435	435
Object	out_buf	out_buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_finish_child(void)

```
....
435.        free(out_buf);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=184
Status	New

Calling free() (line 440) on a variable that was not dynamically allocated (line 440) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	472	472
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_prefixed(void)

```
....
472.        free(buf);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=185
Status	New

Calling free() (line 477) on a variable that was not dynamically allocated (line 477) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	525	525
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_discard_child(void)

```
....
525.        free(buf);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=186
Status	New

Calling free() (line 530) on a variable that was not dynamically allocated (line 530) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	561	561
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_misuse(void)

```
....
561.        free(buf);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=187
Status	New

Calling free() (line 566) on a variable that was not dynamically allocated (line 566) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	586	586
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_asn1(void)

```
....
586.        free(buf);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=188
Status	New

Calling free() (line 566) on a variable that was not dynamically allocated (line 566) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	603	603
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_asn1(void)

```
....
603.        free(buf);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=189
Status	New

Calling free() (line 566) on a variable that was not dynamically allocated (line 566) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	617	617
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_asn1(void)

```
....
617.        free(buf);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=190
Status	New

Calling free() (line 566) on a variable that was not dynamically allocated (line 566) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	640	640
Object	buf	buf

Code Snippet
File Name src-1/bytestringtest.c
Method test_cbb_asn1(void)

```
....
640.         free(buf);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=191
Status	New

Calling free() (line 646) on a variable that was not dynamically allocated (line 646) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	677	677
Object	out	out

Code Snippet
File Name src-1/bytestringtest.c
Method do_indefinite_convert(const char *name, const uint8_t *definite_expected,

```
....
677.         free(out);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=192
Status	New

Calling free() (line 776) on a variable that was not dynamically allocated (line 776) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	806	806
Object	out	out

Code Snippet
File Name src-1/bytestringtest.c
Method test_asn1_uint64(void)

```
....
806.                free(out);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=193
Status	New

Calling free() (line 776) on a variable that was not dynamically allocated (line 776) in file src-1/bytestringtest.c may result with a crash.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	829	829
Object	out	out

Code Snippet
File Name src-1/bytestringtest.c
Method test_asn1_uint64(void)

```
....
829.        free(out);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=194
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	149	149
Object	nm	nm

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

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

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=195
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	150	150
Object	tp	tp

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
150.                free(tp);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=196
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	151	151
Object	cl	cl

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
151.                free(cl);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=197
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	155	155
Object	nm	nm

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
155.                free(nm);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=198
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	156	156
Object	tp	tp

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
156.                free(tp);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=199
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	157	157
Object	cl	cl

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
157.                free(cl);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=200
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	160	160
Object	nm	nm

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
160.        free(nm);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=201
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	161	161
Object	tp	tp

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
161.        free(tp);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=202
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	162	162
Object	cl	cl

Code Snippet
File Name src-1/cachedump.c
Method dump_msg_ref(RES* ssl, struct ub_packed_rrset_key* k)

```
....
162.        free(cl);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=203
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	181	181
Object	nm	nm

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
181.              free(nm);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=204
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	182	182
Object	tp	tp

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
182.                free(tp);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=205
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	183	183
Object	cl	cl

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
183.                free(cl);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=206
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	188	188
Object	nm	nm

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
188.                free(nm);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=207
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	189	189
Object	tp	tp

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
189.                free(tp);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=208
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	190	190
Object	cl	cl

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
190.                free(cl);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=209
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	202	202
Object	nm	nm

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
202.                free(nm);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=210
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	203	203
Object	tp	tp

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
203.                free(tp);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=211
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	204	204
Object	cl	cl

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
204.                free(cl);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=212
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	208	208
Object	nm	nm

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
208.        free(nm);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=213
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	209	209
Object	tp	tp

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
209.        free(tp);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=214
Status	New

Calling free() (line 169) on a variable that was not dynamically allocated (line 169) in file src-1/cachedump.c may result with a crash.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	210	210
Object	cl	cl

Code Snippet
File Name src-1/cachedump.c
Method dump_msg(RES* ssl, struct query_info* k, struct reply_info* d,

```
....
210.        free(cl);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=215
Status	New

Calling free() (line 687) on a variable that was not dynamically allocated (line 687) in file src-1/channels.c may result with a crash.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	724	724
Object	s	s

Code Snippet
File Name src-1/channels.c
Method channel_free(struct ssh *ssh, Channel *c)

```
....
724.                free(s);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=216
Status	New

Calling free() (line 973) on a variable that was not dynamically allocated (line 973) in file src-1/channels.c may result with a crash.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	1015	1015
Object	cp	cp

Code Snippet
File Name src-1/channels.c
Method channel_open_message(struct ssh *ssh)

```
....
1015.                           free(cp);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=217
Status	New

Calling free() (line 973) on a variable that was not dynamically allocated (line 973) in file src-1/channels.c may result with a crash.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	1018	1018
Object	cp	cp

Code Snippet
File Name src-1/channels.c
Method channel_open_message(struct ssh *ssh)

```
....
1018.                       free(cp);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=218
Status	New

Calling free() (line 1762) on a variable that was not dynamically allocated (line 1762) in file src-1/channels.c may result with a crash.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	1807	1807
Object	remote_ipaddr	remote_ipaddr

Code Snippet
File Name src-1/channels.c
Method channel_post_x11_listener(struct ssh *ssh, Channel *c)

```
....
1807.       free(remote_ipaddr);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=219
Status	New

Calling free() (line 1811) on a variable that was not dynamically allocated (line 1811) in file src-1/channels.c may result with a crash.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	1866	1866
Object	local_ipaddr	local_ipaddr

Code Snippet
File Name src-1/channels.c
Method port_open_helper(struct ssh *ssh, Channel *c, char *rtype)

```
....
1866.       free(local_ipaddr);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=220
Status	New

Calling free() (line 2107) on a variable that was not dynamically allocated (line 2107) in file src-1/channels.c may result with a crash.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2142	2142
Object	data	data

Code Snippet
File Name src-1/channels.c
Method channel_handle_wfd(struct ssh *ssh, Channel *c)

```
....
2142.             free(data);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=221
Status	New

Calling free() (line 3032) on a variable that was not dynamically allocated (line 3032) in file src-1/channels.c may result with a crash.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	3172	3172
Object	ctype	ctype

Code Snippet
File Name src-1/channels.c
Method channel_proxy_downstream(struct ssh *ssh, Channel *downstream)

```
....
3172.       free(ctype);
```

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=1050100&projectid=50090&pathid=48
Status	New

The size of the buffer used by rrset_add_rr in old, at line 795 of src-1/authzone.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rrset_add_rr passes to old, at line 795 of src-1/authzone.c, to overwrite the target buffer.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	809	809

Object	old	old

Code Snippet
File Name src-1/authzone.c
Method rrset_add_rr(struct auth_rrset* rrset, uint32_t rr_ttl, uint8_t* rdata,

```
....
809.        memcpy(d, old, sizeof(struct packed_rrset_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=49
Status	New

The size of the buffer used by rrset_moveover_rrsigs in packed_rrset_data, at line 936 of src-1/authzone.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rrset_moveover_rrsigs passes to packed_rrset_data, at line 936 of src-1/authzone.c, to overwrite the target buffer.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	963	963
Object	packed_rrset_data	packed_rrset_data

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
963.        memcpy(d, old, sizeof(struct packed_rrset_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=50
Status	New

The size of the buffer used by rrset_moveover_rrsigs in packed_rrset_data, at line 936 of src-1/authzone.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rrset_moveover_rrsigs passes to packed_rrset_data, at line 936 of src-1/authzone.c, to overwrite the target buffer.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1027	1027

Object	packed_rrset_data	packed_rrset_data

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
1027.       memcpy(sigd, sigold, sizeof(struct packed_rrset_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=51
Status	New

The size of the buffer used by ax_recv in header, at line 98 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_recv passes to header, at line 98 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	171	171
Object	header	header

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
171.        memcpy(&(pdu->ap_header), &header, sizeof(header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=52
Status	New

The size of the buffer used by ax_pdu_add_uint16 in value, at line 1218 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_pdu_add_uint16 passes to value, at line 1218 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1227	1227
Object	value	value

Code Snippet
File Name src-1/ax.c
Method ax_pdu_add_uint16(struct ax *ax, uint16_t value)

```
....
1227.       memcpy(ax->ax_wbuf + ax->ax_wbtlen, &value, sizeof(value));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=53
Status New

The size of the buffer used by ax_pdu_add_uint32 in value, at line 1233 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_pdu_add_uint32 passes to value, at line 1233 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1242	1242
Object	value	value

Code Snippet
File Name src-1/ax.c
Method ax_pdu_add_uint32(struct ax *ax, uint32_t value)

```
....
1242.       memcpy(ax->ax_wbuf + ax->ax_wbtlen, &value, sizeof(value));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=54
Status New

The size of the buffer used by ax_pdu_add_uint64 in value, at line 1248 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_pdu_add_uint64 passes to value, at line 1248 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1257	1257
Object	value	value

Code Snippet
File Name src-1/ax.c

Method	ax_pdu_add_uint64(struct ax *ax, uint64_t value)

```
....
1257.       memcpy(ax->ax_wbuf + ax->ax_wbtlen, &value, sizeof(value));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=55
Status	New

The size of the buffer used by cdioctl in lp, at line 720 of src-1/cd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cdioctl passes to lp, at line 720 of src-1/cd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	782	782
Object	lp	lp

Code Snippet	
File Name	src-1/cd.c
Method	cdioctl(dev_t dev, u_long cmd, caddr_t addr, int flag, struct proc *p)

```
....
782.              memcpy(sc->sc_dk.dk_label, lp, sizeof(*lp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=56
Status	New

The size of the buffer used by cdioctl in th, at line 720 of src-1/cd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cdioctl passes to th, at line 720 of src-1/cd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	881	881
Object	th	th

Code Snippet	
File Name	src-1/cd.c
Method	cdioctl(dev_t dev, u_long cmd, caddr_t addr, int flag, struct proc *p)

```
....
881.                    memcpy(addr, th, sizeof(*th));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=57
Status	New

The size of the buffer used by dvd_read_disckey in Namespace2131791094, at line 1921 of src-1/cd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dvd_read_disckey passes to Namespace2131791094, at line 1921 of src-1/cd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1952	1952
Object	Namespace2131791094	Namespace2131791094

Code Snippet
File Name src-1/cd.c
Method dvd_read_disckey(struct cd_softc *sc, union dvd_struct *s)

```
....
1952.             memcpy(s->disckey.value, buf->data, sizeof(s-
>disckey.value));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=58
Status	New

The size of the buffer used by dtls1_reassemble_fragment in msg_hdr, at line 553 of src-1/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_reassemble_fragment passes to msg_hdr, at line 553 of src-1/d1_both.c, to overwrite the target buffer.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	580	580
Object	msg_hdr	msg_hdr

Code Snippet
File Name src-1/d1_both.c
Method dtls1_reassemble_fragment(SSL *s, struct hm_header_st* msg_hdr, int *ok)

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

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=59
Status	New

The size of the buffer used by dtls1_process_out_of_seq_message in msg_hdr, at line 653 of src-1/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_process_out_of_seq_message passes to msg_hdr, at line 653 of src-1/d1_both.c, to overwrite the target buffer.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	708	708
Object	msg_hdr	msg_hdr

Code Snippet
File Name src-1/d1_both.c
Method dtls1_process_out_of_seq_message(SSL *s, struct hm_header_st* msg_hdr, int *ok)

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

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=60
Status	New

The size of the buffer used by globextend in sb, at line 786 of src-1/glob.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that globextend passes to sb, at line 786 of src-1/glob.c, to overwrite the target buffer.

	Source	Destination
File	src-1/glob.c	src-1/glob.c
Line	851	851
Object	sb	sb

Code Snippet
File Name src-1/glob.c

Method	globextend(const Char *path, glob_t *pglob, struct glob_lim *limitp,

```
....
851.                            sizeof(*sb));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=61
Status	New

The size of the buffer used by gt_record_uc in Namespace351878237, at line 1727 of src-1/i915_gpu_error.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gt_record_uc passes to Namespace351878237, at line 1727 of src-1/i915_gpu_error.c, to overwrite the target buffer.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1737	1737
Object	Namespace351878237	Namespace351878237

Code Snippet	
File Name	src-1/i915_gpu_error.c
Method	gt_record_uc(struct intel_gt_coredump *gt,

```
....
1737.       memcpy(&error_uc->guc_fw, &uc->guc.fw, sizeof(uc->guc.fw));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=62
Status	New

The size of the buffer used by gt_record_uc in Namespace351878237, at line 1727 of src-1/i915_gpu_error.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gt_record_uc passes to Namespace351878237, at line 1727 of src-1/i915_gpu_error.c, to overwrite the target buffer.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1738	1738
Object	Namespace351878237	Namespace351878237

Code Snippet	
File Name	src-1/i915_gpu_error.c
Method	gt_record_uc(struct intel_gt_coredump *gt,

```
....
1738.       memcpy(&error_uc->huc_fw, &uc->huc.fw, sizeof(uc->huc.fw));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=63
Status	New

The size of the buffer used by gt_record_info in intel_gt_info, at line 1913 of src-1/i915_gpu_error.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gt_record_info passes to intel_gt_info, at line 1913 of src-1/i915_gpu_error.c, to overwrite the target buffer.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1915	1915
Object	intel_gt_info	intel_gt_info

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void gt_record_info(struct intel_gt_coredump *gt)

```
....
1915.       memcpy(&gt->info, &gt->_gt->info, sizeof(struct
intel_gt_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=64
Status	New

The size of the buffer used by capture_gen in ->, at line 1975 of src-1/i915_gpu_error.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that capture_gen passes to ->, at line 1975 of src-1/i915_gpu_error.c, to overwrite the target buffer.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1989	1989
Object	->	->

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void capture_gen(struct i915_gpu_coredump *error)

```
....
1989.               sizeof(error->device_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=65
Status	New

The size of the buffer used by capture_gen in ->, at line 1975 of src-1/i915_gpu_error.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that capture_gen passes to ->, at line 1975 of src-1/i915_gpu_error.c, to overwrite the target buffer.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	1992	1992
Object	->	->

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void capture_gen(struct i915_gpu_coredump *error)

```
....
1992.               sizeof(error->runtime_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=66
Status	New

The size of the buffer used by ip6_savecontrol in in6_addr, at line 1015 of src-1/ip6_input.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ip6_savecontrol passes to in6_addr, at line 1015 of src-1/ip6_input.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	1032	1032
Object	in6_addr	in6_addr

Code Snippet
File Name src-1/ip6_input.c
Method ip6_savecontrol(struct inpcb *in6p, struct mbuf *m, struct mbuf **mp)

```
....
1032.             memcpy(&pi6.ipi6_addr, &ip6->ip6_dst, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=67
Status	New

The size of the buffer used by enternewpgrp in ->, at line 268 of src-1/kern_proc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that enternewpgrp passes to ->, at line 268 of src-1/kern_proc.c, to overwrite the target buffer.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	285	285
Object	->	->

Code Snippet
File Name src-1/kern_proc.c
Method enternewpgrp(struct process *pr, struct pgrp *pgrp, struct session *newsess)

```
....
285.                 sizeof(newsess->s_login));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=68
Status	New

The size of the buffer used by main in buf2, at line 3 of src-1/memcpy-6.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to buf2, at line 3 of src-1/memcpy-6.c, to overwrite the target buffer.

	Source	Destination
File	src-1/memcpy-6.c	src-1/memcpy-6.c
Line	6	6
Object	buf2	buf2

Code Snippet
File Name src-1/memcpy-6.c
Method int main(int argc, char **argv) {

```
....
6.    memcpy(buf, buf2, sizeof buf2);
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=69
Status	New

The size of the buffer used by pf_modulate_sack in sack, at line 3136 of src-1/pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pf_modulate_sack passes to sack, at line 3136 of src-1/pf.c, to overwrite the target buffer.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	3165	3165
Object	sack	sack

Code Snippet
File Name src-1/pf.c
Method pf_modulate_sack(struct pf_pdesc *pd, struct pf_state_peer *dst)

```
....
3165.                    memcpy(&opt[i], &sack, sizeof(sack));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=70
Status	New

The size of the buffer used by pf_build_tcp in in6_addr, at line 3177 of src-1/pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pf_build_tcp passes to in6_addr, at line 3177 of src-1/pf.c, to overwrite the target buffer.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	3253	3253
Object	in6_addr	in6_addr

Code Snippet
File Name src-1/pf.c
Method pf_build_tcp(const struct pf_rule *r, sa_family_t af,

```
....
3253.              memcpy(&h6->ip6_src, &saddr->v6, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=71
Status	New

The size of the buffer used by pf_build_tcp in in6_addr, at line 3177 of src-1/pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pf_build_tcp passes to in6_addr, at line 3177 of src-1/pf.c, to overwrite the target buffer.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	3254	3254
Object	in6_addr	in6_addr

Code Snippet
File Name src-1/pf.c
Method pf_build_tcp(const struct pf_rule *r, sa_family_t af,

```
....
3254.              memcpy(&h6->ip6_dst, &daddr->v6, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=72
Status	New

The size of the buffer used by pf_create_state in ->, at line 4495 of src-1/pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pf_create_state passes to ->, at line 4495 of src-1/pf.c, to overwrite the target buffer.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	4652	4652
Object	->	->

Code Snippet
File Name src-1/pf.c
Method pf_create_state(struct pf_pdesc *pd, struct pf_rule *r, struct pf_rule *a,

```
....
4652.       memcpy(&st->match_rules, rules, sizeof(st->match_rules));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=73
Status	New

The size of the buffer used by pf_walk_option6 in ->, at line 6920 of src-1/pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pf_walk_option6 passes to ->, at line 6920 of src-1/pf.c, to overwrite the target buffer.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	6967	6967
Object	->	->

Code Snippet
File Name src-1/pf.c
Method pf_walk_option6(struct pf_pdesc *pd, struct ip6_hdr *h, int off, int end,

```
....
6967.                       sizeof(pd->jumbolen));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=74
Status	New

The size of the buffer used by xid_map_enter in ->, at line 766 of src-1/print-nfs.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xid_map_enter passes to ->, at line 766 of src-1/print-nfs.c, to overwrite the target buffer.

	Source	Destination
File	src-1/print-nfs.c	src-1/print-nfs.c
Line	784	784
Object	->	->

Code Snippet
File Name src-1/print-nfs.c
Method xid_map_enter(const struct rpc_msg *rp, const u_char *bp)

```
....
784.                memcpy(&xmep->client, &ip->ip_src, sizeof(ip-
>ip_src));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=75
Status	New

The size of the buffer used by xid_map_enter in ->, at line 766 of src-1/print-nfs.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xid_map_enter passes to ->, at line 766 of src-1/print-nfs.c, to overwrite the target buffer.

	Source	Destination
File	src-1/print-nfs.c	src-1/print-nfs.c
Line	785	785
Object	->	->

Code Snippet
File Name src-1/print-nfs.c
Method xid_map_enter(const struct rpc_msg *rp, const u_char *bp)

```
....
785.                memcpy(&xmep->server, &ip->ip_dst, sizeof(ip-
>ip_dst));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=76
Status	New

The size of the buffer used by xid_map_enter in ->, at line 766 of src-1/print-nfs.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xid_map_enter passes to ->, at line 766 of src-1/print-nfs.c, to overwrite the target buffer.

	Source	Destination
File	src-1/print-nfs.c	src-1/print-nfs.c
Line	789	789
Object	->	->

Code Snippet
File Name src-1/print-nfs.c
Method xid_map_enter(const struct rpc_msg *rp, const u_char *bp)

```
....
789.                memcpy(&xmep->client, &ip6->ip6_src, sizeof(ip6-
>ip6_src));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=77
Status	New

The size of the buffer used by xid_map_enter in ->, at line 766 of src-1/print-nfs.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xid_map_enter passes to ->, at line 766 of src-1/print-nfs.c, to overwrite the target buffer.

	Source	Destination
File	src-1/print-nfs.c	src-1/print-nfs.c
Line	790	790
Object	->	->

Code Snippet
File Name src-1/print-nfs.c
Method xid_map_enter(const struct rpc_msg *rp, const u_char *bp)

```
....
790.                memcpy(&xmep->server, &ip6->ip6_dst, sizeof(ip6-
>ip6_dst));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=78
Status	New

The size of the buffer used by prefixlen2mask6 in s6, at line 1830 of src-1/relayd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prefixlen2mask6 passes to s6, at line 1830 of src-1/relayd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1845	1845
Object	s6	s6

Code Snippet
File Name src-1/relayd.c
Method prefixlen2mask6(u_int8_t prefixlen, u_int32_t *mask)

```
....
1845.       memcpy(mask, &s6, sizeof(s6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=79
Status	New

The size of the buffer used by rdata2sockaddr in ->, at line 567 of src-1/respip.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rdata2sockaddr passes to ->, at line 567 of src-1/respip.c, to overwrite the target buffer.

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	578	578
Object	->	->

Code Snippet
File Name src-1/respip.c
Method rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i,

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

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=80
Status	New

The size of the buffer used by rdata2sockaddr in ->, at line 567 of src-1/respip.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rdata2sockaddr passes to ->, at line 567 of src-1/respip.c, to overwrite the target buffer.

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	587	587
Object	->	->

Code Snippet
File Name src-1/respip.c
Method rdata2sockaddr(const struct packed_rrset_data* rd, uint16_t rtype, size_t i,

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

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=81
Status	New

The size of the buffer used by ssl3_get_client_hello in tls13_downgrade_12, at line 793 of src-1/ssl_srvr.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssl3_get_client_hello passes to tls13_downgrade_12, at line 793 of src-1/ssl_srvr.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ssl_srvr.c	src-1/ssl_srvr.c
Line	1072	1072
Object	tls13_downgrade_12	tls13_downgrade_12

Code Snippet
File Name src-1/ssl_srvr.c
Method ssl3_get_client_hello(SSL *s)

```
....
1072.                       sizeof(tls13_downgrade_12));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=82
Status	New

The size of the buffer used by ssl3_get_client_hello in tls13_downgrade_11, at line 793 of src-1/ssl_srvr.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssl3_get_client_hello passes to tls13_downgrade_11, at line 793 of src-1/ssl_srvr.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ssl_srvr.c	src-1/ssl_srvr.c
Line	1076	1076
Object	tls13_downgrade_11	tls13_downgrade_11

Code Snippet
File Name src-1/ssl_srvr.c
Method ssl3_get_client_hello(SSL *s)

```
....
1076.                          sizeof(tls13_downgrade_11));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=83
Status	New

The size of the buffer used by dm_dp_mst_get_modes in ->, at line 291 of src-1/amdgpu_dm_mst_types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dm_dp_mst_get_modes passes to ->, at line 291 of src-1/amdgpu_dm_mst_types.c, to overwrite the target buffer.

	Source	Destination
File	src-1/amdgpu_dm_mst_types.c	src-1/amdgpu_dm_mst_types.c
Line	373	373
Object	->	->

Code Snippet
File Name src-1/amdgpu_dm_mst_types.c
Method static int dm_dp_mst_get_modes(struct drm_connector *connector)

```
....
373.                                    0, sizeof(aconnector->dc_sink->dsc_caps));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=84
Status	New

The size of the buffer used by dm_dp_mst_get_modes in ->, at line 291 of src-1/amdgpu_dm_mst_types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dm_dp_mst_get_modes passes to ->, at line 291 of src-1/amdgpu_dm_mst_types.c, to overwrite the target buffer.

	Source	Destination
File	src-1/amdgpu_dm_mst_types.c	src-1/amdgpu_dm_mst_types.c
Line	377	377
Object	->	->

Code Snippet
File Name src-1/amdgpu_dm_mst_types.c
Method static int dm_dp_mst_get_modes(struct drm_connector *connector)

```
....
377.                                    0, sizeof(aconnector-
>mst_downstream_port_present));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=85
Status	New

The size of the buffer used by test_write_bytes in input, at line 873 of src-1/bytestringtest.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_write_bytes passes to input, at line 873 of src-1/bytestringtest.c, to overwrite the target buffer.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	883	883
Object	input	input

Code Snippet
File Name src-1/bytestringtest.c
Method test_write_bytes(void)

```
....
883.        memset(tmp, 100, sizeof(input));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=86
Status	New

The size of the buffer used by dtls1_get_message in hm_header_st, at line 372 of src-1/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_get_message passes to hm_header_st, at line 372 of src-1/d1_both.c, to overwrite the target buffer.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	396	396
Object	hm_header_st	hm_header_st

Code Snippet
File Name src-1/d1_both.c
Method dtls1_get_message(SSL *s, int st1, int stn, int mt, long max)

```
....
396.        memset(msg_hdr, 0, sizeof(struct hm_header_st));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=87
Status	New

The size of the buffer used by dtls1_get_message in hm_header_st, at line 372 of src-1/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_get_message passes to hm_header_st, at line 372 of src-1/d1_both.c, to overwrite the target buffer.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	420	420
Object	hm_header_st	hm_header_st

Code Snippet
File Name src-1/d1_both.c
Method dtls1_get_message(SSL *s, int st1, int stn, int mt, long max)

```
....
420.        memset(msg_hdr, 0, sizeof(struct hm_header_st));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=88
Status	New

The size of the buffer used by calculate_ss in delta_sigma_data, at line 645 of src-1/dce_clock_source.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that calculate_ss passes to delta_sigma_data, at line 645 of src-1/dce_clock_source.c, to overwrite the target buffer.

	Source	Destination
File	src-1/dce_clock_source.c	src-1/dce_clock_source.c
Line	666	666
Object	delta_sigma_data	delta_sigma_data

Code Snippet
File Name src-1/dce_clock_source.c
Method static bool calculate_ss(

```
....
666.        memset(ds_data, 0, sizeof(struct delta_sigma_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=89
Status	New

The size of the buffer used by ip6_input_if in sockaddr_in6, at line 358 of src-1/ip6_input.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ip6_input_if passes to sockaddr_in6, at line 358 of src-1/ip6_input.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	520	520
Object	sockaddr_in6	sockaddr_in6

Code Snippet
File Name src-1/ip6_input.c
Method ip6_input_if(struct mbuf **mp, int *offp, int nxt, int af, struct ifnet *ifp)

```
....
520.        memset(&sin6, 0, sizeof(struct sockaddr_in6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=90
Status	New

The size of the buffer used by pf_state_export in pfsync_state, at line 1280 of src-1/pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pf_state_export passes to pfsync_state, at line 1280 of src-1/pf.c, to overwrite the target buffer.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1284	1284
Object	pfsync_state	pfsync_state

Code Snippet
File Name src-1/pf.c
Method pf_state_export(struct pfsync_state *sp, struct pf_state *st)

```
....
1284.       memset(sp, 0, sizeof(struct pfsync_state));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=91
Status	New

The size of the buffer used by pf_get_divert in pf_divert, at line 6781 of src-1/pf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pf_get_divert passes to pf_divert, at line 6781 of src-1/pf.c, to overwrite the target buffer.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	6790	6790
Object	pf_divert	pf_divert

Code Snippet
File Name src-1/pf.c
Method pf_get_divert(struct mbuf *m)

```
....
6790.             memset(mtag + 1, 0, sizeof(struct pf_divert));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=92
Status	New

The size of the buffer used by respip_copy_rrset in ->, at line 488 of src-1/respip.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that respip_copy_rrset passes to ->, at line 488 of src-1/respip.c, to overwrite the target buffer.

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	502	502
Object	->	->

Code Snippet
File Name src-1/respip.c
Method respip_copy_rrset(const struct ub_packed_rrset_key* key, struct regional* region)

```
....
502.        memset(&ck->entry, 0, sizeof(ck->entry));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=93
Status	New

The size of the buffer used by ssl3_connect in ->, at line 199 of src-1/ssl_clnt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssl3_connect passes to ->, at line 199 of src-1/ssl_clnt.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ssl_clnt.c	src-1/ssl_clnt.c
Line	277	277
Object	->	->

Code Snippet
File Name src-1/ssl_clnt.c
Method ssl3_connect(SSL *s)

```
....
277.                                sizeof(s->s3->client_random));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=94
Status	New

The size of the buffer used by cdgetdisklabel in ->, at line 1111 of src-1/cd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cdgetdisklabel passes to ->, at line 1111 of src-1/cd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1126	1126
Object	->	->

Code Snippet
File Name src-1/cd.c
Method cdgetdisklabel(dev_t dev, struct cd_softc *sc, struct disklabel *lp,

```
....
1126.             strncpy(lp->d_typename, "ATAPI CD-ROM", sizeof(lp-
>d_typename));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=95
Status	New

The size of the buffer used by cdgetdisklabel in ->, at line 1111 of src-1/cd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cdgetdisklabel passes to ->, at line 1111 of src-1/cd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1129	1129
Object	->	->

Code Snippet
File Name src-1/cd.c
Method cdgetdisklabel(dev_t dev, struct cd_softc *sc, struct disklabel *lp,

```
....
1129.             strncpy(lp->d_typename, "SCSI CD-ROM", sizeof(lp-
>d_typename));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=96
Status	New

The size of the buffer used by cdgetdisklabel in ->, at line 1111 of src-1/cd.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cdgetdisklabel passes to ->, at line 1111 of src-1/cd.c, to overwrite the target buffer.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1133	1133
Object	->	->

Code Snippet
File Name src-1/cd.c
Method cdgetdisklabel(dev_t dev, struct cd_softc *sc, struct disklabel *lp,

```
....
1133.       strncpy(lp->d_packname, "fictitious", sizeof(lp-
>d_packname));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=97
Status	New

The size of the buffer used by add_modifier in size, at line 128 of src-1/amdgpu_dm_plane.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that add_modifier passes to size, at line 128 of src-1/amdgpu_dm_plane.c, to overwrite the target buffer.

	Source	Destination
File	src-1/amdgpu_dm_plane.c	src-1/amdgpu_dm_plane.c
Line	143	143
Object	size	size

Code Snippet
File Name src-1/amdgpu_dm_plane.c
Method static void add_modifier(uint64_t **mods, uint64_t *size, uint64_t *cap, uint64_t mod)

```
....
143.              memcpy(new_mods, *mods, sizeof(uint64_t) * *size);
```

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=1050100&projectid=50090&pathid=1680
Status	New

The variable declared in amdgpu_state at src-1/amdgpu_dm_plane.c in line 1319 is not initialized when it is used by amdgpu_state at src-1/amdgpu_dm_plane.c in line 1319.

	Source	Destination
File	src-1/amdgpu_dm_plane.c	src-1/amdgpu_dm_plane.c

Line	1321	1326
Object	amdgpu_state	amdgpu_state

Code Snippet
File Name src-1/amdgpu_dm_plane.c
Method static void dm_drm_plane_reset(struct drm_plane *plane)

```
....
1321.       struct dm_plane_state *amdgpu_state = NULL;
....
1326.       amdgpu_state = kzalloc(sizeof(*amdgpu_state), GFP_KERNEL);
```

Use of Zero Initialized Pointer\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1681
Status New

The variable declared in b at src-1/asn1_item.c in line 575 is not initialized when it is used by b at src-1/asn1_item.c in line 575.

	Source	Destination
File	src-1/asn1_item.c	src-1/asn1_item.c
Line	577	586
Object	b	b

Code Snippet
File Name src-1/asn1_item.c
Method ASN1_item_d2i_bio(const ASN1_ITEM *it, BIO *in, void *x)

```
....
577.        BUF_MEM *b = NULL;
....
586.        p = (const unsigned char *)b->data;
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1682
Status New

The variable declared in delete_list at src-1/authzone.c in line 2201 is not initialized when it is used by delete_list at src-1/authzone.c in line 2201.

	Source	Destination

File	src-1/authzone.c	src-1/authzone.c
Line	2204	2214
Object	delete_list	delete_list

Code Snippet
File Name src-1/authzone.c
Method az_delete_deleted_zones(struct auth_zones* az)

```
....
2204.       struct auth_zone* delete_list = NULL, *next;
....
2214.                   delete_list = z;
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1683
Status New

The variable declared in cp at src-1/authzone.c in line 5442 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	5473	5496
Object	cp	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5473.            xfr->task_transfer->cp = NULL;
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1684
Status New

The variable declared in next at src-1/authzone.c in line 3965 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3977	5496
Object	next	cp

Code Snippet
File Name src-1/authzone.c
Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3977.             m->next = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.             xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1685
Status New

The variable declared in list at src-1/authzone.c in line 3965 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3967	5496
Object	list	cp

Code Snippet
File Name src-1/authzone.c
Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3967.       struct auth_master* list = NULL, *last = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1686
Status	New

The variable declared in scan_specific at src-1/authzone.c in line 4136 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4148	5496
Object	scan_specific	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_transfer_nextmaster(struct auth_xfer* xfr)

```
....
4148.            xfr->task_transfer->scan_specific = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1687
Status	New

The variable declared in scan_addr at src-1/authzone.c in line 3989 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3992	5496

Object	scan_addr	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_start_lookups(struct auth_xfer* xfr)

```
....
3992.       xfr->task_transfer->scan_addr = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1688
Status	New

The variable declared in scan_target at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4056	5496
Object	scan_target	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4056.                   xfr->task_transfer->scan_target = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1689
Status	New

The variable declared in scan_addr at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4057	5496
Object	scan_addr	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4057.                   xfr->task_transfer->scan_addr = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.             xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1690
Status	New

The variable declared in scan_specific at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4065	5496
Object	scan_specific	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4065.       xfr->task_transfer->scan_specific = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1691
Status	New

The variable declared in scan_addr at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4066	5496
Object	scan_addr	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4066.       xfr->task_transfer->scan_addr = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1692
Status	New

The variable declared in cp at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6318	5496
Object	cp	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6318.       xfr->task_probe->cp = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1693
Status	New

The variable declared in timer at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6315	5496
Object	timer	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6315.       xfr->task_probe->timer = NULL;
```

File Name src-1/authzone.c

Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1694
Status	New

The variable declared in worker at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6320	5496
Object	worker	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6320.       xfr->task_probe->worker = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.            xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1695
Status	New

The variable declared in env at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c

Line	6321	5496
Object	env	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6321.       xfr->task_probe->env = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.             xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1696
Status	New

The variable declared in next at src-1/authzone.c in line 6022 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6028	5496
Object	next	cp

Code Snippet
File Name src-1/authzone.c
Method xfer_link_data(sldns_buffer* pkt, struct auth_xfer* xfr)

```
....
6028.       e->next = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5496.             xfr->task_transfer->cp = outnet_comm_point_for_http(
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1697
Status	New

The variable declared in cp at src-1/authzone.c in line 5442 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	5473	5528
Object	cp	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5473.             xfr->task_transfer->cp = NULL;
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env->outnet,
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1698
Status	New

The variable declared in auth_name at src-1/authzone.c in line 5442 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	5447	5528
Object	auth_name	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5447.       char *auth_name = NULL;
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1699
Status	New

The variable declared in next at src-1/authzone.c in line 3965 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3977	5528
Object	next	cp

Code Snippet

File Name src-1/authzone.c

Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3977.            m->next = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1700
Status	New

The variable declared in list at src-1/authzone.c in line 3965 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination

File	src-1/authzone.c	src-1/authzone.c
Line	3967	5528
Object	list	cp

Code Snippet
File Name src-1/authzone.c
Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3967.       struct auth_master* list = NULL, *last = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1701
Status	New

The variable declared in scan_specific at src-1/authzone.c in line 4136 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4148	5528
Object	scan_specific	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_nextmaster(struct auth_xfer* xfr)

```
....
4148.           xfr->task_transfer->scan_specific = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1702
Status	New

The variable declared in scan_addr at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4057	5528
Object	scan_addr	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4057.                   xfr->task_transfer->scan_addr = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1703
Status	New

The variable declared in scan_target at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c

Line	4056	5528
Object	scan_target	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4056.                   xfr->task_transfer->scan_target = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1704
Status	New

The variable declared in scan_addr at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4066	5528
Object	scan_addr	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4066.       xfr->task_transfer->scan_addr = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1705
Status	New

The variable declared in scan_addr at src-1/authzone.c in line 3989 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3992	5528
Object	scan_addr	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_transfer_start_lookups(struct auth_xfer* xfr)

```
....
3992.       xfr->task_transfer->scan_addr = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1706
Status	New

The variable declared in scan_specific at src-1/authzone.c in line 4050 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	4065	5528
Object	scan_specific	cp

Code Snippet

File Name src-1/authzone.c
Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4065.       xfr->task_transfer->scan_specific = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1707
Status	New

The variable declared in timer at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6315	5528
Object	timer	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6315.       xfr->task_probe->timer = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 29:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1708
Status	New

The variable declared in cp at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6318	5528
Object	cp	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6318.       xfr->task_probe->cp = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env->outnet,
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1709
Status	New

The variable declared in worker at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6320	5528
Object	worker	cp

Code Snippet
File Name src-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6320.       xfr->task_probe->worker = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1710
Status	New

The variable declared in env at src-1/authzone.c in line 6311 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6321	5528
Object	env	cp

Code Snippet

File Name src-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6321.       xfr->task_probe->env = NULL;
```

File Name src-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.       xfr->task_transfer->cp = outnet_comm_point_for_tcp(env-
>outnet,
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1711

Status	New

The variable declared in next at src-1/authzone.c in line 6022 is not initialized when it is used by cp at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	6028	5528
Object	next	cp

Code Snippet
File Name src-1/authzone.c
Method xfer_link_data(sldns_buffer* pkt, struct auth_xfer* xfr)

```
....
6028.        e->next = NULL;
```

File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5528.        xfr->task_transfer->cp = outnet_comm_point_for_tcp(env->outnet,
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1712
Status	New

The variable declared in auth_name at src-1/authzone.c in line 5442 is not initialized when it is used by auth_name at src-1/authzone.c in line 5442.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	5447	5531
Object	auth_name	auth_name

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5447.       char *auth_name = NULL;
....
5531.             auth_name != NULL, auth_name);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1713
Status	New

The variable declared in srl at src-1/ax.c in line 98 is not initialized when it is used by srl at src-1/ax.c in line 98.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	104	324
Object	srl	srl

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
104.        struct ax_pdu_searchrangelist *srl = NULL;
....
324.                    sr = reallocarray(srl->ap_sr, srl->ap_nsr,
sizeof(*sr));
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1714
Status	New

The variable declared in srl at src-1/ax.c in line 98 is not initialized when it is used by srl at src-1/ax.c in line 98.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	104	324
Object	srl	srl

Code Snippet
File Name src-1/ax.c

Method	ax_recv(struct ax *ax)

```
....
104.        struct ax_pdu_searchrangelist *srl = NULL;
....
324.                    sr = reallocarray(srl->ap_sr, srl->ap_nsr,
sizeof(*sr));
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1715
Status	New

The variable declared in srl at src-1/ax.c in line 98 is not initialized when it is used by srl at src-1/ax.c in line 98.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	104	323
Object	srl	srl

Code Snippet	
File Name	src-1/ax.c
Method	ax_recv(struct ax *ax)

```
....
104.        struct ax_pdu_searchrangelist *srl = NULL;
....
323.                    srl->ap_nsr++;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1716
Status	New

The variable declared in out_buf at src-1/bytestringtest.c in line 391 is not initialized when it is used by out_buf at src-1/bytestringtest.c in line 391.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	395	409
Object	out_buf	out_buf

Code Snippet

File Name	src-1/bytestringtest.c
Method	test_cbb_fixed(void)

```
....
395.        uint8_t *out_buf = NULL;
....
409.        ret = (out_buf == buf && out_size == 1 && buf[0] == 1);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1717
Status	New

The variable declared in out_buf at src-1/bytestringtest.c in line 420 is not initialized when it is used by out_buf at src-1/bytestringtest.c in line 420.

	Source	Destination
File	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	423	432
Object	out_buf	out_buf

Code Snippet

File Name	src-1/bytestringtest.c
Method	test_cbb_finish_child(void)

```
....
423.        uint8_t *out_buf = NULL;
....
432.        ret = (out_size == 1 && out_buf[0] == 0);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1718
Status	New

The variable declared in audio at src-1/cd.c in line 1163 is not initialized when it is used by audio at src-1/cd.c in line 1163.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1166	1174
Object	audio	audio

Code Snippet

File Name src-1/cd.c
Method cd_setchan(struct cd_softc *sc, int p0, int p1, int p2, int p3, int flags)

```
....
1166.       struct cd_audio_page          *audio = NULL;
....
1174.           (void **)&audio, sizeof(*audio), flags, &big);
```

Use of Zero Initialized Pointer\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1719
Status New

The variable declared in audio at src-1/cd.c in line 1196 is not initialized when it is used by audio at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1215
Object	audio	audio

Code Snippet
File Name src-1/cd.c
Method cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1215.             arg->vol[3] = audio->port[3].volume;
```

Use of Zero Initialized Pointer\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1720
Status New

The variable declared in audio at src-1/cd.c in line 1196 is not initialized when it is used by audio at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1214
Object	audio	audio

Code Snippet

File Name	src-1/cd.c
Method	cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1214.             arg->vol[2] = audio->port[2].volume;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1721
Status	New

The variable declared in audio at src-1/cd.c in line 1196 is not initialized when it is used by audio at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1213
Object	audio	audio

Code Snippet

File Name	src-1/cd.c
Method	cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1213.             arg->vol[1] = audio->port[1].volume;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1722
Status	New

The variable declared in audio at src-1/cd.c in line 1196 is not initialized when it is used by audio at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1212
Object	audio	audio

Code Snippet

File Name src-1/cd.c
Method cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1212.             arg->vol[0] = audio->port[0].volume;
```

Use of Zero Initialized Pointer\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1723
Status New

The variable declared in audio at src-1/cd.c in line 1196 is not initialized when it is used by audio at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1207
Object	audio	audio

Code Snippet
File Name src-1/cd.c
Method cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1207.            (void **)&audio, sizeof(*audio), flags, &big);
```

Use of Zero Initialized Pointer\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1724
Status New

The variable declared in audio at src-1/cd.c in line 1223 is not initialized when it is used by audio at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1250
Object	audio	audio

Code Snippet

File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1250.           (void **)&audio, sizeof(*audio), flags, &big);
```

Use of Zero Initialized Pointer\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1725
Status New

The variable declared in audio at src-1/cd.c in line 1223 is not initialized when it is used by audio at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1247
Object	audio	audio

Code Snippet
File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1247.       mask_volume[3] = audio->port[3].volume;
```

Use of Zero Initialized Pointer\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1726
Status New

The variable declared in audio at src-1/cd.c in line 1223 is not initialized when it is used by audio at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1246
Object	audio	audio

Code Snippet

File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1246.       mask_volume[2] = audio->port[2].volume;
```

Use of Zero Initialized Pointer\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1727
Status New

The variable declared in audio at src-1/cd.c in line 1223 is not initialized when it is used by audio at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1245
Object	audio	audio

Code Snippet
File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1245.       mask_volume[1] = audio->port[1].volume;
```

Use of Zero Initialized Pointer\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1728
Status New

The variable declared in audio at src-1/cd.c in line 1223 is not initialized when it is used by audio at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1244
Object	audio	audio

Code Snippet

File Name	src-1/cd.c
Method	cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1244.       mask_volume[0] = audio->port[0].volume;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1729
Status	New

The variable declared in audio at src-1/cd.c in line 1223 is not initialized when it is used by audio at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1236
Object	audio	audio

Code Snippet	
File Name	src-1/cd.c
Method	cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1236.           sizeof(*audio), flags, &big);
```

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=1050100&projectid=50090&pathid=660
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c

Line	726	726
Object	newvalue	newvalue

Code Snippet
File Name src-1/relayd.c
Method kv_extend(struct kvtree *keys, struct kv *kv, char *value)

```
....
726.                if (asprintf(&newvalue, "%s%s", kv->kv_value, value)
== -1)
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=661
Status New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	689	689
Object	key	key

Code Snippet
File Name src-1/relayd.c
Method kv_setkey(struct kv *kv, char *fmt, ...)

```
....
689.        ret = vasprintf(&key, fmt, ap);
```

Memory Leak\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=662
Status New

	Source	Destination
File	src-1/dsa_ossl.c	src-1/dsa_ossl.c
Line	208	208
Object	ret	ret

Code Snippet
File Name src-1/dsa_ossl.c
Method dsa_do_sign(const unsigned char *dgst, int dlen, DSA *dsa)

```
....
208.        if ((ret = DSA_SIG_new()) == NULL) {
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=663
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	858	858
Object	do_macro_ctime	do_macro_ctime

Code Snippet
File Name src-1/replay.c
Method macro_expand(rbtree_type* store, struct replay_runtime* runtime, char** text)

```
....
858.                    return do_macro_ctime(buf+6);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=664
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	860	860
Object	do_macro_range	do_macro_range

Code Snippet
File Name src-1/replay.c
Method macro_expand(rbtree_type* store, struct replay_runtime* runtime, char** text)

```
....
860.                    return do_macro_range(buf+6);
```

Memory Leak\Path 6:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=665
Status	New

	Source	Destination
File	src-1/asan_mac_test.cpp	src-1/asan_mac_test.cpp
Line	189	189
Object	mem	mem

Code Snippet
File Name src-1/asan_mac_test.cpp
Method void *TSDAllocWorker(void *test_key) {

```
....
189.      void *mem = malloc(10);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=666
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	7143	7143
Object	result	result

Code Snippet
File Name src-1/authzone.c
Method dup_all(char* str)

```
....
7143.       char* result = strdup(str);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=667
Status	New

	Source	Destination
File	src-1/dtstream.c	src-1/dtstream.c
Line	451	451

Object	item	item

Code Snippet
File Name src-1/dtstream.c
Method int dt_io_thread_register_queue(struct dt_io_thread* dtio,

```
....
451.        struct dt_io_list_item* item = malloc(sizeof(*item));
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=668
Status New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	72	72
Object	ipsecmod_env	ipsecmod_env

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_init(struct module_env* env, int id)

```
....
72.   struct ipsecmod_env* ipsecmod_env = (struct
ipsecmod_env*)calloc(1,
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=669
Status New

	Source	Destination
File	src-1/asn1_item.c	src-1/asn1_item.c
Line	300	300
Object	buf_out	buf_out

Code Snippet
File Name src-1/asn1_item.c
Method ASN1_item_sign_ctx(const ASN1_ITEM *it, X509_ALGOR *algor1, X509_ALGOR *algor2,

```
....
300.        if ((buf_out = malloc(out_len)) == NULL) {
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=670
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	566	566
Object	zonefile	zonefile

Code Snippet
File Name src-1/authzone.c
Method auth_zone_set_zonefile(struct auth_zone* z, char* zonefile)

```
....
566.              z->zonefile = strdup(zonefile);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=671
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	801	801
Object	d	d

Code Snippet
File Name src-1/authzone.c
Method rrset_add_rr(struct auth_rrset* rrset, uint32_t rr_ttl, uint8_t* rdata,

```
....
801.        d = (struct packed_rrset_data*)calloc(1,
packed_rrset_sizeof(old)
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=672
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	954	954
Object	d	d

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
954.         d = (struct packed_rrset_data*)calloc(1,
packed_rrset_sizeof(old)
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=673
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1017	1017
Object	sigd	sigd

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
1017.        sigd = (struct packed_rrset_data*)calloc(1,
packed_rrset_sizeof(sigold)
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=674
Status	New

	Source	Destination

File	src-1/authzone.c	src-1/authzone.c
Line	5625	5625
Object	a	a

Code Snippet
File Name src-1/authzone.c
Method xfr_master_add_addrs(struct auth_master* m, struct ub_packed_rrset_key* rrset,

```
....
5625.             a = (struct auth_addr*)calloc(1, sizeof(*a));
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=675
Status New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	7110	7110
Object	m	m

Code Snippet
File Name src-1/authzone.c
Method auth_master_new(struct auth_master*** list)

```
....
7110.       m = (struct auth_master*)calloc(1, sizeof(*m));
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=676
Status New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	7257	7257
Object	host	host

Code Snippet
File Name src-1/authzone.c

Method	xfer_set_masters(struct auth_master** list, struct config_auth* c,

```
....
7257.             m->host = strdup(p->str);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=677
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	7267	7267
Object	host	host

Code Snippet	
File Name	src-1/authzone.c
Method	xfer_set_masters(struct auth_master** list, struct config_auth* c,

```
....
7267.             m->host = strdup(p->str);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=678
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	74	74
Object	ax_rbuf	ax_rbuf

Code Snippet	
File Name	src-1/ax.c
Method	ax_new(int fd)

```
....
74.   if ((ax->ax_rbuf = malloc(ax->ax_rbsize)) == NULL)
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=679
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	168	168
Object	pdu	pdu

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
168.        if ((pdu = calloc(1, sizeof(*pdu))) == NULL)
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=680
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	1469	1469
Object	aos_string	aos_string

Code Snippet
File Name src-1/ax.c
Method ax_pdutoostring(struct ax_pdu_header *header,

```
....
1469.       if ((ostring->aos_string = malloc(ostring->aos_slen + 1)) ==
NULL)
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=681
Status	New

	Source	Destination
File	src-1/buffer.c	src-1/buffer.c

Line	78	78
Object	ret	ret

Code Snippet
File Name src-1/buffer.c
Method BUF_MEM_new(void)

```
....
78.    if ((ret = calloc(1, sizeof(BUF_MEM))) == NULL) {
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=682
Status New

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	408	408
Object	ad	ad

Code Snippet
File Name src-1/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
408.         ad = (struct packed_rrset_data*)malloc(s);
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=683
Status New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	231	231
Object	sc	sc

Code Snippet
File Name src-1/channels.c
Method channel_init_channels(struct ssh *ssh)

```
....
231.        if ((sc = calloc(1, sizeof(*sc))) == NULL)
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=684
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2440	2440
Object	pre	pre

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2440.       if ((pre = calloc(SSH_CHANNEL_MAX_TYPE, sizeof(*pre))) ==
NULL ||
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=685
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2441	2441
Object	post	post

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2441.           (post = calloc(SSH_CHANNEL_MAX_TYPE, sizeof(*post))) ==
NULL)
```

Memory Leak\Path 27:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=686
Status	New

	Source	Destination
File	src-1/cms_enc.c	src-1/cms_enc.c
Line	132	132
Object	tkey	tkey

Code Snippet
File Name src-1/cms_enc.c
Method cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
132.                tkey = malloc(tkeylen);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=687
Status	New

	Source	Destination
File	src-1/cms_enc.c	src-1/cms_enc.c
Line	213	213
Object	key	key

Code Snippet
File Name src-1/cms_enc.c
Method cms_EncryptedContent_init(CMS_EncryptedContentInfo *ec,

```
....
213.                if ((ec->key = malloc(keylen)) == NULL) {
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=688
Status	New

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c

Line	176	176
Object	frag	frag

Code Snippet
File Name src-1/d1_both.c
Method dtls1_hm_fragment_new(unsigned long frag_len, int reassembly)

```
....
176.        if ((frag = calloc(1, sizeof(*frag))) == NULL)
```

Memory Leak\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=689
Status New

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	180	180
Object	fragment	fragment

Code Snippet
File Name src-1/d1_both.c
Method dtls1_hm_fragment_new(unsigned long frag_len, int reassembly)

```
....
180.              if ((frag->fragment = calloc(1, frag_len)) == NULL)
```

Memory Leak\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=690
Status New

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	186	186
Object	reassembly	reassembly

Code Snippet
File Name src-1/d1_both.c
Method dtls1_hm_fragment_new(unsigned long frag_len, int reassembly)

```
....
186.              if ((frag->reassembly = calloc(1,
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=691
Status	New

	Source	Destination
File	src-1/dir.c	src-1/dir.c
Line	307	307
Object	d	d

Code Snippet
File Name src-1/dir.c
Method read_directory(struct PathEntry *p)

```
....
307.          if ((d = opendir(p->name)) == NULL)
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=692
Status	New

	Source	Destination
File	src-1/drm_drv.c	src-1/drm_drv.c
Line	1217	1217
Object	busid	busid

Code Snippet
File Name src-1/drm_drv.c
Method drm_attach_pci(const struct drm_driver *driver, struct pci_attach_args *pa,

```
....
1217.         arg.busid = malloc(arg.busid_len + 1, M_DRM, M_NOWAIT);
```

Memory Leak\Path 34:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=693
Status	New

	Source	Destination
File	src-1/drm_drv.c	src-1/drm_drv.c
Line	1351	1351
Object	self	self

Code Snippet
File Name src-1/drm_drv.c
Method drm_attach(struct device *parent, struct device *self, void *aux)

```
....
1351.                    dev->pdev->bus->self = malloc(sizeof(struct
pci_dev),
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=694
Status	New

	Source	Destination
File	src-1/dtstream.c	src-1/dtstream.c
Line	361	361
Object	socket_path	socket_path

Code Snippet
File Name src-1/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
361.              dtio->socket_path = strdup(nm);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=695
Status	New

	Source	Destination
File	src-1/dtstream.c	src-1/dtstream.c

Line	374	374
Object	ip_str	ip_str

Code Snippet
File Name src-1/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
374.              dtio->ip_str = strdup(cfg->dnstap_ip);
```

Memory Leak\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=696
Status New

	Source	Destination
File	src-1/dtstream.c	src-1/dtstream.c
Line	386	386
Object	tls_server_name	tls_server_name

Code Snippet
File Name src-1/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
386.                    dtio->tls_server_name = strdup(
```

Memory Leak\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=697
Status New

	Source	Destination
File	src-1/dtstream.c	src-1/dtstream.c
Line	399	399
Object	client_key_file	client_key_file

Code Snippet
File Name src-1/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
399.                    dtio->client_key_file = strdup(
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=698
Status	New

	Source	Destination
File	src-1/dtstream.c	src-1/dtstream.c
Line	415	415
Object	client_cert_file	client_cert_file

Code Snippet
File Name src-1/dtstream.c
Method int dt_io_thread_apply_cfg(struct dt_io_thread* dtio, struct config_file *cfg)

```
....
415.                    dtio->client_cert_file = strdup(
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=699
Status	New

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	156	156
Object	rti	rti

Code Snippet
File Name src-1/igmp.c
Method rti_fill(struct in_multi *inm)

```
....
156.        rti = malloc(sizeof(*rti), M_MRTABLE, M_WAITOK);
```

Memory Leak\Path 41:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=700
Status	New

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	175	175
Object	rti	rti

Code Snippet
File Name src-1/igmp.c
Method rti_find(struct ifnet *ifp)

```
....
175.        rti = malloc(sizeof(*rti), M_MRTABLE, M_NOWAIT);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=701
Status	New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	1017	1017
Object	log_str	log_str

Code Snippet
File Name src-1/ixfrcreate.c
Method static void ixfr_create_finishup(struct ixfr_create* ixfrcr,

```
....
1017.       store->data->log_str = strdup(log_buf);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=702
Status	New

	Source	Destination
File	src-1/ls.c	src-1/ls.c
Line	516	516

Object	np	np

Code Snippet
File Name src-1/ls.c
Method display(FTSENT *p, FTSENT *list)

```
....
516.                            if ((np = malloc(sizeof(NAMES) +
```

Memory Leak\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=703
Status New

	Source	Destination
File	src-1/packet.c	src-1/packet.c
Line	106	106
Object	recv_buf	recv_buf

Code Snippet
File Name src-1/packet.c
Method recv_packet(int fd, short event, void *bula)

```
....
106.                if ((recv_buf = malloc(READ_BUF_SIZE)) == NULL)
```

Memory Leak\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=704
Status New

	Source	Destination
File	src-1/pvkfmt.c	src-1/pvkfmt.c
Line	859	859
Object	p	p

Code Snippet
File Name src-1/pvkfmt.c
Method i2b_PVK(unsigned char **out, EVP_PKEY*pk, int enclevel, pem_password_cb *cb,

```
....
859.        start = p = malloc(outlen);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=705
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	177	177
Object	env	env

Code Snippet
File Name src-1/relayd.c
Method main(int argc, char *argv[])

```
....
177.        if ((env = calloc(1, sizeof(*env))) == NULL ||
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=706
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	178	178
Object	ps	ps

Code Snippet
File Name src-1/relayd.c
Method main(int argc, char *argv[])

```
....
178.            (ps = calloc(1, sizeof(*ps))) == NULL)
```

Memory Leak\Path 48:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=707
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	627	627
Object	kv_key	kv_key

Code Snippet
File Name src-1/relayd.c
Method kv_add(struct kvtree *keys, char *key, char *value, int unique)

```
....
627.        if ((kv->kv_key = strdup(key)) == NULL)
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=708
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	630	630
Object	kv_value	kv_value

Code Snippet
File Name src-1/relayd.c
Method kv_add(struct kvtree *keys, char *key, char *value, int unique)

```
....
630.            (kv->kv_value = strdup(value)) == NULL)
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=709
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	731	731

Object	kv_value	kv_value

Code Snippet
File Name src-1/relayd.c
Method kv_extend(struct kvtree *keys, struct kv *kv, char *value)

```
....
731.        } else if ((kv->kv_value = strdup(value)) == NULL)
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=746
Status	New

The variable declared in ctx at src-1/amdgpu_ctx.c in line 858 is not initialized when it is used by entities at src-1/amdgpu_ctx.c in line 858.

	Source	Destination
File	src-1/amdgpu_ctx.c	src-1/amdgpu_ctx.c
Line	860	875
Object	ctx	entities

Code Snippet
File Name src-1/amdgpu_ctx.c
Method long amdgpu_ctx_mgr_entity_flush(struct amdgpu_ctx_mgr *mgr, long timeout)

```
....
860.        struct amdgpu_ctx *ctx;
....
875.                            entity = &ctx->entities[i][j]->entity;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=747
Status	New

The variable declared in ctx at src-1/amdgpu_ctx.c in line 858 is not initialized when it is used by entities at src-1/amdgpu_ctx.c in line 858.

	Source	Destination
File	src-1/amdgpu_ctx.c	src-1/amdgpu_ctx.c
Line	860	872
Object	ctx	entities

Code Snippet
File Name src-1/amdgpu_ctx.c
Method long amdgpu_ctx_mgr_entity_flush(struct amdgpu_ctx_mgr *mgr, long timeout)

```
....
860.        struct amdgpu_ctx *ctx;
....
872.                            if (!ctx->entities[i][j])
```

Use of Uninitialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=748
Status New

The variable declared in ra at src-1/igmp.c in line 112 is not initialized when it is used by ipopt_list at src-1/igmp.c in line 112.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	114	134
Object	ra	ipopt_list

Code Snippet
File Name src-1/igmp.c
Method igmp_init(void)

```
....
114.        struct ipoption *ra;
....
134.        ra->ipopt_list[0] = IPOPT_RA;
```

Use of Uninitialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=749
Status New

The variable declared in ra at src-1/igmp.c in line 112 is not initialized when it is used by s_addr at src-1/igmp.c in line 112.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	114	133
Object	ra	s_addr

Code Snippet
File Name src-1/igmp.c
Method igmp_init(void)

```
....
114.        struct ipoption *ra;
....
133.        ra->ipopt_dst.s_addr = INADDR_ANY;
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=750
Status	New

The variable declared in ra at src-1/igmp.c in line 112 is not initialized when it is used by ipopt_list at src-1/igmp.c in line 112.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	114	135
Object	ra	ipopt_list

Code Snippet
File Name src-1/igmp.c
Method igmp_init(void)

```
....
114.        struct ipoption *ra;
....
135.        ra->ipopt_list[1] = 0x04;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=751
Status	New

The variable declared in ra at src-1/igmp.c in line 112 is not initialized when it is used by ipopt_list at src-1/igmp.c in line 112.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	114	136
Object	ra	ipopt_list

Code Snippet
File Name src-1/igmp.c
Method igmp_init(void)

```
....
114.        struct ipoption *ra;
....
136.        ra->ipopt_list[2] = 0x00;
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=752
Status	New

The variable declared in ra at src-1/igmp.c in line 112 is not initialized when it is used by ipopt_list at src-1/igmp.c in line 112.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	114	137
Object	ra	ipopt_list

Code Snippet
File Name src-1/igmp.c
Method igmp_init(void)

```
....
114.        struct ipoption *ra;
....
137.        ra->ipopt_list[3] = 0x00;
```

Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=753
Status	New

The variable declared in ra at src-1/igmp.c in line 112 is not initialized when it is used by ipopt_list at src-1/igmp.c in line 112.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	114	138
Object	ra	ipopt_list

Code Snippet
File Name src-1/igmp.c
Method igmp_init(void)

```
....
114.        struct ipoption *ra;
....
138.        router_alert->m_len = sizeof(ra->ipopt_dst) + ra-
>ipopt_list[1];
```

Use of Uninitialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=754
Status New

The variable declared in rti at src-1/igmp.c in line 579 is not initialized when it is used by rti_age at src-1/igmp.c in line 579.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	581	587
Object	rti	rti_age

Code Snippet
File Name src-1/igmp.c
Method igmp_slowtimo(void)

```
....
581.        struct router_info *rti;
....
587.                    ++rti->rti_age >= IGMP_AGE_THRESHOLD) {
```

Use of Uninitialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=755
Status New

The variable declared in rti at src-1/igmp.c in line 579 is not initialized when it is used by rti_type at src-1/igmp.c in line 579.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	581	586
Object	rti	rti_type

Code Snippet
File Name src-1/igmp.c
Method igmp_slowtimo(void)

```
....
581.        struct router_info *rti;
....
586.              if (rti->rti_type == IGMP_v1_ROUTER &&
```

Use of Uninitialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=756
Status New

The variable declared in rti at src-1/igmp.c in line 579 is not initialized when it is used by rti_type at src-1/igmp.c in line 579.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	581	588
Object	rti	rti_type

Code Snippet
File Name src-1/igmp.c
Method igmp_slowtimo(void)

```
....
581.        struct router_info *rti;
....
588.                    rti->rti_type = IGMP_v2_ROUTER;
```

Use of Uninitialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=757
Status New

The variable declared in igmp at src-1/igmp.c in line 596 is not initialized when it is used by igmp_type at src-1/igmp.c in line 596.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	600	631
Object	igmp	igmp_type

Code Snippet
File Name src-1/igmp.c
Method igmp_sendpkt(struct ifnet *ifp, struct in_multi *inm, int type,

```
....
600.         struct igmp *igmp;
....
631.         igmp->igmp_type = type;
```

Use of Uninitialized Pointer\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=758
Status New

The variable declared in igmp at src-1/igmp.c in line 596 is not initialized when it is used by igmp at src-1/igmp.c in line 596.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	600	600
Object	igmp	igmp

Code Snippet
File Name src-1/igmp.c
Method igmp_sendpkt(struct ifnet *ifp, struct in_multi *inm, int type,

```
....
600.         struct igmp *igmp;
```

Use of Uninitialized Pointer\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=759
Status New

The variable declared in igmp at src-1/igmp.c in line 596 is not initialized when it is used by igmp_code at src-1/igmp.c in line 596.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	600	632
Object	igmp	igmp_code

Code Snippet
File Name src-1/igmp.c
Method igmp_sendpkt(struct ifnet *ifp, struct in_multi *inm, int type,

```
....
600.        struct igmp *igmp;
....
632.        igmp->igmp_code = 0;
```

Use of Uninitialized Pointer\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=760
Status New

The variable declared in igmp at src-1/igmp.c in line 596 is not initialized when it is used by igmp_group at src-1/igmp.c in line 596.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	600	633
Object	igmp	igmp_group

Code Snippet
File Name src-1/igmp.c
Method igmp_sendpkt(struct ifnet *ifp, struct in_multi *inm, int type,

```
....
600.        struct igmp *igmp;
....
633.        igmp->igmp_group = inm->inm_addr;
```

Use of Uninitialized Pointer\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=761
Status New

The variable declared in igmp at src-1/igmp.c in line 596 is not initialized when it is used by igmp_cksum at src-1/igmp.c in line 596.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	600	634
Object	igmp	igmp_cksum

Code Snippet
File Name src-1/igmp.c
Method igmp_sendpkt(struct ifnet *ifp, struct in_multi *inm, int type,

```
....
600.        struct igmp *igmp;
....
634.        igmp->igmp_cksum = 0;
```

Use of Uninitialized Pointer\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=762
Status New

The variable declared in igmp at src-1/igmp.c in line 596 is not initialized when it is used by igmp_cksum at src-1/igmp.c in line 596.

	Source	Destination
File	src-1/igmp.c	src-1/igmp.c
Line	600	635
Object	igmp	igmp_cksum

Code Snippet
File Name src-1/igmp.c
Method igmp_sendpkt(struct ifnet *ifp, struct in_multi *inm, int type,

```
....
600.        struct igmp *igmp;
....
635.        igmp->igmp_cksum = in_cksum(m, IGMP_MINLEN);
```

Use of Uninitialized Pointer\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=763
Status New

The variable declared in ip6 at src-1/ip6_input.c in line 223 is not initialized when it is used by ip6_nxt at src-1/ip6_input.c in line 223.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	245	249
Object	ip6	ip6_nxt

Code Snippet
File Name src-1/ip6_input.c
Method ip6intr(void)

```
....
245.                    struct ip6_hdr *ip6;
....
249.                    nxt = ip6->ip6_nxt;
```

Use of Uninitialized Pointer\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=764
Status New

The variable declared in hbh at src-1/ip6_input.c in line 634 is not initialized when it is used by ip6h_nxt at src-1/ip6_input.c in line 634.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	650	681
Object	hbh	ip6h_nxt

Code Snippet
File Name src-1/ip6_input.c
Method ip6_hbhchcheck(struct mbuf **mp, int *offp, int *oursp)

```
....
650.                struct ip6_hbh *hbh;
....
681.                nxt = hbh->ip6h_nxt;
```

Use of Uninitialized Pointer\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=765
Status New

The variable declared in hbh at src-1/ip6_input.c in line 634 is not initialized when it is used by hbh at src-1/ip6_input.c in line 634.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	650	677
Object	hbh	hbh

Code Snippet
File Name src-1/ip6_input.c
Method ip6_hbhchcheck(struct mbuf **mp, int *offp, int *oursp)

```
....
650.              struct ip6_hbh *hbh;
....
677.              if (hbh == NULL) {
```

Use of Uninitialized Pointer\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=766
Status New

The variable declared in ip6 at src-1/ip6_input.c in line 839 is not initialized when it is used by ip6_plen at src-1/ip6_input.c in line 839.

	Source	Destination
File	src-1/ip6_input.c	src-1/ip6_input.c
Line	842	898
Object	ip6	ip6_plen

Code Snippet
File Name src-1/ip6_input.c
Method ip6_process_hopopts(struct mbuf **mp, u_int8_t *opthead, int hbhlen,

```
....
842.        struct ip6_hdr *ip6;
....
898.                    if (ip6->ip6_plen) {
```

Use of Uninitialized Pointer\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=767
Status New

The variable declared in uip at src-1/kern_proc.c in line 123 is not initialized when it is used by uip at src-1/kern_proc.c in line 123.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	125	133
Object	uip	uip

Code Snippet
File Name src-1/kern_proc.c
Method uid_find(uid_t uid)

```
....
125.        struct uidinfo *uip, *nuip;
....
133.        if (uip)
```

Use of Uninitialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=768
Status	New

The variable declared in uip at src-1/kern_proc.c in line 123 is not initialized when it is used by ui_uid at src-1/kern_proc.c in line 123.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	125	131
Object	uip	ui_uid

Code Snippet
File Name src-1/kern_proc.c
Method uid_find(uid_t uid)

```
....
125.        struct uidinfo *uip, *nuip;
....
131.              if (uip->ui_uid == uid)
```

Use of Uninitialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=769
Status	New

The variable declared in uip at src-1/kern_proc.c in line 123 is not initialized when it is used by uip at src-1/kern_proc.c in line 123.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	125	134
Object	uip	uip

Code Snippet
File Name src-1/kern_proc.c
Method uid_find(uid_t uid)

```
....
125.        struct uidinfo *uip, *nuip;
....
134.              return (uip);
```

Use of Uninitialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=770
Status	New

The variable declared in uip at src-1/kern_proc.c in line 123 is not initialized when it is used by ui_uid at src-1/kern_proc.c in line 123.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	125	139
Object	uip	ui_uid

Code Snippet
File Name src-1/kern_proc.c
Method uid_find(uid_t uid)

```
....
125.        struct uidinfo *uip, *nuip;
....
139.              if (uip->ui_uid == uid)
```

Use of Uninitialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=771
Status	New

The variable declared in uip at src-1/kern_proc.c in line 123 is not initialized when it is used by uip at src-1/kern_proc.c in line 123.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	125	141
Object	uip	uip

Code Snippet
File Name src-1/kern_proc.c
Method uid_find(uid_t uid)

```
....
125.        struct uidinfo *uip, *nuip;
....
141.        if (uip) {
```

Use of Uninitialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=772
Status	New

The variable declared in uip at src-1/kern_proc.c in line 123 is not initialized when it is used by uip at src-1/kern_proc.c in line 123.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	125	143
Object	uip	uip

Code Snippet
File Name src-1/kern_proc.c
Method uid_find(uid_t uid)

```
....
125.        struct uidinfo *uip, *nuip;
....
143.              return (uip);
```

Use of Uninitialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=773
Status	New

The variable declared in p at src-1/kern_proc.c in line 192 is not initialized when it is used by p at src-1/kern_proc.c in line 192.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	194	198
Object	p	p

Code Snippet
File Name src-1/kern_proc.c
Method tfind(pid_t tid)

```
....
194.        struct proc *p;
....
198.                    return (p);
```

Use of Uninitialized Pointer\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=774
Status New

The variable declared in p at src-1/kern_proc.c in line 192 is not initialized when it is used by p_tid at src-1/kern_proc.c in line 192.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	194	197
Object	p	p_tid

Code Snippet
File Name src-1/kern_proc.c
Method tfind(pid_t tid)

```
....
194.        struct proc *p;
....
197.              if (p->p_tid == tid)
```

Use of Uninitialized Pointer\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=775
Status New

The variable declared in pr at src-1/kern_proc.c in line 224 is not initialized when it is used by pr at src-1/kern_proc.c in line 224.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	226	230
Object	pr	pr

Code Snippet
File Name src-1/kern_proc.c
Method prfind(pid_t pid)

```
....
226.        struct process *pr;
....
230.                    return (pr);
```

Use of Uninitialized Pointer\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=776
Status New

The variable declared in pr at src-1/kern_proc.c in line 224 is not initialized when it is used by ps_pid at src-1/kern_proc.c in line 224.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	226	229
Object	pr	ps_pid

Code Snippet
File Name src-1/kern_proc.c
Method prfind(pid_t pid)

```
....
226.        struct process *pr;
....
229.              if (pr->ps_pid == pid)
```

Use of Uninitialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=777
Status New

The variable declared in pgrp at src-1/kern_proc.c in line 238 is not initialized when it is used by pgrp at src-1/kern_proc.c in line 238.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	240	240
Object	pgrp	pgrp

Code Snippet
File Name src-1/kern_proc.c
Method pgfind(pid_t pgid)

```
....
240.        struct pgrp *pgrp;
```

Use of Uninitialized Pointer\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=778
Status New

The variable declared in pgrp at src-1/kern_proc.c in line 238 is not initialized when it is used by pgrp at src-1/kern_proc.c in line 238.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	240	237
Object	pgrp	pgrp

Code Snippet
File Name src-1/kern_proc.c
Method pgfind(pid_t pgid)

```
....
240.        struct pgrp *pgrp;
....
237.  struct pgrp *
```

Use of Uninitialized Pointer\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=779
Status New

The variable declared in pgrp at src-1/kern_proc.c in line 238 is not initialized when it is used by pg_id at src-1/kern_proc.c in line 238.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	240	243
Object	pgrp	pg_id

Code Snippet
File Name src-1/kern_proc.c
Method pgfind(pid_t pgid)

```
....
240.        struct pgrp *pgrp;
....
243.                if (pgrp->pg_id == pgid)
```

Use of Uninitialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=780
Status	New

The variable declared in pgrp at src-1/kern_proc.c in line 238 is not initialized when it is used by pgrp at src-1/kern_proc.c in line 238.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	240	244
Object	pgrp	pgrp

Code Snippet
File Name src-1/kern_proc.c
Method pgfind(pid_t pgid)

```
....
240.        struct pgrp *pgrp;
....
244.                    return (pgrp);
```

Use of Uninitialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=781
Status	New

The variable declared in pr at src-1/kern_proc.c in line 252 is not initialized when it is used by pr at src-1/kern_proc.c in line 252.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	254	258
Object	pr	pr

Code Snippet
File Name src-1/kern_proc.c
Method zombiefind(pid_t pid)

```
....
254.        struct process *pr;
....
258.                    return (pr);
```

Use of Uninitialized Pointer\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=782
Status New

The variable declared in pr at src-1/kern_proc.c in line 252 is not initialized when it is used by ps_pid at src-1/kern_proc.c in line 252.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	254	257
Object	pr	ps_pid

Code Snippet
File Name src-1/kern_proc.c
Method zombiefind(pid_t pid)

```
....
254.        struct process *pr;
....
257.              if (pr->ps_pid == pid)
```

Use of Uninitialized Pointer\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=783
Status New

The variable declared in cur at src-1/kfd_packet_manager.c in line 121 is not initialized when it is used by qpd at src-1/kfd_packet_manager.c in line 121.

	Source	Destination
File	src-1/kfd_packet_manager.c	src-1/kfd_packet_manager.c
Line	129	150
Object	cur	qpd

Code Snippet
File Name src-1/kfd_packet_manager.c
Method static int pm_create_runlist_ib(struct packet_manager *pm,

```
....
129.        struct device_process_node *cur;
....
150.                qpd = cur->qpd;
```

Use of Uninitialized Pointer\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=784
Status New

The variable declared in sni at src-1/pf.c in line 655 is not initialized when it is used by sn at src-1/pf.c in line 655.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	657	661
Object	sni	sn

Code Snippet
File Name src-1/pf.c
Method pf_get_src_node(struct pf_state *st, enum pf_sn_types type)

```
....
657.        struct pf_sn_item *sni;
....
661.                    return (sni->sn);
```

Use of Uninitialized Pointer\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=785
Status New

The variable declared in sni at src-1/pf.c in line 655 is not initialized when it is used by sn at src-1/pf.c in line 655.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	657	660
Object	sni	sn

Code Snippet
File Name src-1/pf.c
Method pf_get_src_node(struct pf_state *st, enum pf_sn_types type)

```
....
657.        struct pf_sn_item *sni;
....
660.              if (sni->sn->type == type)
```

Use of Uninitialized Pointer\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=786
Status New

The variable declared in si at src-1/pf.c in line 1121 is not initialized when it is used by si_st at src-1/pf.c in line 1121.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1125	1182
Object	si	si_st

Code Snippet
File Name src-1/pf.c
Method pf_find_state(struct pf_pdesc *pd, struct pf_state_key_cmp *key,

```
....
1125.       struct pf_state_item    *si;
....
1182.             struct pf_state *sist = si->si_st;
```

Use of Uninitialized Pointer\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=787
Status New

The variable declared in si at src-1/pf.c in line 1750 is not initialized when it is used by si_st at src-1/pf.c in line 1750.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1752	1759
Object	si	si_st

Code Snippet
File Name src-1/pf.c
Method pf_remove_divert_state(struct pf_state_key *sk)

```
....
1752.       struct pf_state_item    *si;
....
1759.             struct pf_state *sist = si->si_st;
```

Use of Uninitialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=788
Status	New

The variable declared in sni at src-1/pf.c in line 7389 is not initialized when it is used by bytes at src-1/pf.c in line 7389.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	7408	7412
Object	sni	bytes

Code Snippet
File Name src-1/pf.c
Method pf_counters_inc(int action, struct pf_pdesc *pd, struct pf_state *st,

```
....
7408.                   struct pf_sn_item *sni;
....
7412.                         sni->sn->bytes[dirndx] += pd->tot_len;
```

Use of Uninitialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=789
Status	New

The variable declared in sni at src-1/pf.c in line 7389 is not initialized when it is used by packets at src-1/pf.c in line 7389.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	7408	7411
Object	sni	packets

Code Snippet
File Name src-1/pf.c
Method pf_counters_inc(int action, struct pf_pdesc *pd, struct pf_state *st,

```
....
7408.                   struct pf_sn_item *sni;
....
7411.                         sni->sn->packets[dirndx]++;
```

Use of Uninitialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=790
Status	New

The variable declared in host at src-1/relayd.c in line 1047 is not initialized when it is used by host at src-1/relayd.c in line 1047.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1050	1050
Object	host	host

Code Snippet
File Name src-1/relayd.c
Method host_find(struct relayd *env, objid_t id)

```
....
1050.       struct host *host;
```

Use of Uninitialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=791
Status	New

The variable declared in host at src-1/relayd.c in line 1047 is not initialized when it is used by host at src-1/relayd.c in line 1047.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1050	1046
Object	host	host

Code Snippet
File Name src-1/relayd.c
Method host_find(struct relayd *env, objid_t id)

```
....
1050.       struct host *host;
....
1046.  struct host *
```

Use of Uninitialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=792
Status	New

The variable declared in host at src-1/relayd.c in line 1047 is not initialized when it is used by conf at src-1/relayd.c in line 1047.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1050	1054
Object	host	conf

Code Snippet
File Name src-1/relayd.c
Method host_find(struct relayd *env, objid_t id)

```
....
1050.       struct host *host;
....
1054.                   if (host->conf.id == id)
```

Use of Uninitialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=793
Status	New

The variable declared in host at src-1/relayd.c in line 1047 is not initialized when it is used by host at src-1/relayd.c in line 1047.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1050	1055
Object	host	host

Code Snippet
File Name src-1/relayd.c
Method host_find(struct relayd *env, objid_t id)

```
....
1050.       struct host *host;
....
1055.                           return (host);
```

Use of Uninitialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=794
Status	New

The variable declared in table at src-1/relayd.c in line 1060 is not initialized when it is used by table at src-1/relayd.c in line 1060.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1062	1062
Object	table	table

Code Snippet
File Name src-1/relayd.c
Method table_find(struct relayd *env, objid_t id)

```
....
1062.       struct table      *table;
```

Use of Uninitialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=795
Status	New

The variable declared in table at src-1/relayd.c in line 1060 is not initialized when it is used by table at src-1/relayd.c in line 1060.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1062	1059
Object	table	table

Code Snippet
File Name src-1/relayd.c
Method table_find(struct relayd *env, objid_t id)

```
....
1062.       struct table      *table;
....
1059.  struct table *
```

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=1050100&projectid=50090&pathid=304
Status New

The function kMallocSize in src-1/asan_mac_test.cpp at line 224 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	src-1/asan_mac_test.cpp	src-1/asan_mac_test.cpp
Line	228	228
Object	kMallocSize	kMallocSize

Code Snippet
File Name src-1/asan_mac_test.cpp
Method TEST(AddressSanitizerMac, Mstats) {

```
....
228.    void *alloc = Ident(malloc(kMallocSize));
```

Wrong Size t Allocation\Path 2:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=305
Status	New

The function s in src-1/cachedump.c at line 381 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	408	408
Object	s	s

Code Snippet
File Name src-1/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
408.        ad = (struct packed_rrset_data*)malloc(s);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=306
Status	New

The function tkeylen in src-1/cms_enc.c at line 71 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	src-1/cms_enc.c	src-1/cms_enc.c
Line	132	132
Object	tkeylen	tkeylen

Code Snippet
File Name src-1/cms_enc.c
Method cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
132.                tkey = malloc(tkeylen);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=307
Status	New

The function keylen in src-1/cms_enc.c at line 208 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	src-1/cms_enc.c	src-1/cms_enc.c
Line	213	213
Object	keylen	keylen

Code Snippet
File Name src-1/cms_enc.c
Method cms_EncryptedContent_init(CMS_EncryptedContentInfo *ec,

```
....
213.              if ((ec->key = malloc(keylen)) == NULL) {
```

Wrong Size t Allocation\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=308
Status New

The function eklen in src-1/cms_env.c at line 357 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	src-1/cms_env.c	src-1/cms_env.c
Line	397	397
Object	eklen	eklen

Code Snippet
File Name src-1/cms_env.c
Method cms_RecipientInfo_ktri_encrypt(CMS_ContentInfo *cms, CMS_RecipientInfo *ri)

```
....
397.          ek = malloc(eklen);
```

Wrong Size t Allocation\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=309
Status New

The function eklen in src-1/cms_env.c at line 423 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	src-1/cms_env.c	src-1/cms_env.c
Line	476	476
Object	eklen	eklen

Code Snippet
File Name src-1/cms_env.c
Method cms_RecipientInfo_ktri_decrypt(CMS_ContentInfo *cms, CMS_RecipientInfo *ri)

```
....
476.         ek = malloc(eklen);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=310
Status	New

The function strsize in src-1/drm_drv.c at line 1883 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	src-1/drm_drv.c	src-1/drm_drv.c
Line	1893	1893
Object	strsize	strsize

Code Snippet
File Name src-1/drm_drv.c
Method drm_dmamem_alloc(bus_dma_tag_t dmat, bus_size_t size, bus_size_t alignment,

```
....
1893.        mem = malloc(strsize, M_DRM, M_NOWAIT | M_ZERO);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=311
Status	New

The function len in src-1/glob.c at line 786 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	src-1/glob.c	src-1/glob.c
Line	860	860
Object	len	len

Code Snippet
File Name src-1/glob.c
Method globextend(const Char *path, glob_t *pglob, struct glob_lim *limitp,

```
....
860.        if ((copy = malloc(len)) != NULL) {
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=312
Status	New

The function buflen in src-1/pvkfmt.c at line 807 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	src-1/pvkfmt.c	src-1/pvkfmt.c
Line	824	824
Object	buflen	buflen

Code Snippet
File Name src-1/pvkfmt.c
Method b2i_PVK_bio(BIO *in, pem_password_cb *cb, void *u)

```
....
824.        buf = malloc(buflen);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=313
Status	New

The function pms_len in src-1/ssl_srvr.c at line 1643 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	src-1/ssl_srvr.c	src-1/ssl_srvr.c
Line	1670	1670

Object	pms_len	pms_len

Code Snippet
File Name src-1/ssl_srvr.c
Method ssl3_get_client_kex_rsa(SSL *s, CBS *cbs)

```
....
1670.       if ((pms = malloc(pms_len)) == NULL)
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=314
Status	New

The function n in src-1/unifdef.c at line 1543 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	src-1/unifdef.c	src-1/unifdef.c
Line	1550	1550
Object	n	n

Code Snippet
File Name src-1/unifdef.c
Method xstrdup(const char *start, const char *end)

```
....
1550.       s = (char *)malloc(n);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=315
Status	New

The function len in src-1/telnet.c at line 1300 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	src-1/telnet.c	src-1/telnet.c
Line	1330	1330
Object	len	len

Code Snippet	
File Name	src-1/telnet.c
Method	env_opt_add(char *ep)

```
....
1330.             p = realloc(opt_reply, len);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=316
Status	New

The function frag_len in src-1/d1_both.c at line 172 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	src-1/d1_both.c	src-1/d1_both.c
Line	180	180
Object	frag_len	frag_len

Code Snippet	
File Name	src-1/d1_both.c
Method	dtls1_hm_fragment_new(unsigned long frag_len, int reassembly)

```
....
180.             if ((frag->fragment = calloc(1, frag_len)) == NULL)
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=317
Status	New

The function n in src-1/glob.c at line 461 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	src-1/glob.c	src-1/glob.c
Line	563	563
Object	n	n

Code Snippet	
File Name	src-1/glob.c
Method	glob0(const Char *pattern, glob_t *pglob, struct glob_lim *limitp)

```
....
563.                    if ((path_stat = calloc(n, sizeof(*path_stat)))
== NULL)
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=318
Status	New

The function slen in src-1/ipsecmod.c at line 215 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	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	218	218
Object	slen	slen

Code Snippet
File Name src-1/ipsecmod.c
Method ipseckey_has_safe_characters(char* s, size_t slen) {

```
....
218.        gateway = (char*)calloc(slen, sizeof(char));
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=319
Status	New

The function len in src-1/relayd.c at line 1453 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	src-1/relayd.c	src-1/relayd.c
Line	1458	1458
Object	len	len

Code Snippet
File Name src-1/relayd.c
Method expand_string(char *label, size_t len, const char *srch, const char *repl)

```
....
1458.       if ((tmp = calloc(1, len)) == NULL) {
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=320
Status	New

The function signature_len in src-1/ssl_clnt.c at line 2104 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	src-1/ssl_clnt.c	src-1/ssl_clnt.c
Line	2142	2142
Object	signature_len	signature_len

Code Snippet
File Name src-1/ssl_clnt.c
Method ssl3_send_client_verify_sigalgs(SSL *s, EVP_PKEY *pkey,

```
....
2142.       if ((signature = calloc(1, signature_len)) == NULL) {
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=321
Status	New

The function signature_len in src-1/ssl_clnt.c at line 2241 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	src-1/ssl_clnt.c	src-1/ssl_clnt.c
Line	2279	2279
Object	signature_len	signature_len

Code Snippet
File Name src-1/ssl_clnt.c
Method ssl3_send_client_verify_gost(SSL *s, EVP_PKEY *pkey, CBB *cert_verify)

```
....
2279.       if ((signature = calloc(1, signature_len)) == NULL) {
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=322
Status	New

The function signature_len in src-1/ssl_srvr.c at line 1432 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	src-1/ssl_srvr.c	src-1/ssl_srvr.c
Line	1533	1533
Object	signature_len	signature_len

Code Snippet
File Name src-1/ssl_srvr.c
Method ssl3_send_server_key_exchange(SSL *s)

```
....
1533.                   if ((signature = calloc(1, signature_len)) ==
NULL) {
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=323
Status	New

The function enc_session_max_len in src-1/ssl_srvr.c at line 2329 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	src-1/ssl_srvr.c	src-1/ssl_srvr.c
Line	2385	2385
Object	enc_session_max_len	enc_session_max_len

Code Snippet
File Name src-1/ssl_srvr.c
Method ssl3_send_newsession_ticket(SSL *s)

```
....
2385.             if ((enc_session = calloc(1, enc_session_max_len)) ==
NULL)
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=324
Status	New

The function len in src-1/server.c at line 489 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	src-1/server.c	src-1/server.c
Line	510	510
Object	len	len

Code Snippet
File Name src-1/server.c
Method docmdspecial(void)

```
....
510.                          env = xmalloc(len);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=325
Status	New

The function len in src-1/server.c at line 489 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	src-1/server.c	src-1/server.c
Line	515	515
Object	len	len

Code Snippet
File Name src-1/server.c
Method docmdspecial(void)

```
....
515.                            env = xrealloc(env, len);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=326
Status	New

The function len in src-1/server.c at line 489 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	src-1/server.c	src-1/server.c
Line	525	525
Object	len	len

Code Snippet
File Name src-1/server.c
Method docmdspecial(void)

```
....
525.                            env = xrealloc(env, len);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=327
Status	New

The function num in src-1/authzone.c at line 7124 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	src-1/authzone.c	src-1/authzone.c
Line	7129	7129
Object	num	num

Code Snippet
File Name src-1/authzone.c
Method dup_prefix(char* str, size_t num)

```
....
7129.       result = (char*)malloc(num+1);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=328
Status	New

The function rdatalen in src-1/authzone.c at line 795 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	src-1/authzone.c	src-1/authzone.c
Line	803	803
Object	rdatalen	rdatalen

Code Snippet
File Name src-1/authzone.c
Method rrset_add_rr(struct auth_rrset* rrset, uint32_t rr_ttl, uint8_t* rdata,

```
....
803.              + rdatalen);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=329
Status	New

The function sigsz in src-1/authzone.c at line 936 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	src-1/authzone.c	src-1/authzone.c
Line	956	956
Object	sigsz	sigsz

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
956.                + sigsz);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=330
Status	New

The function sigsz in src-1/authzone.c at line 936 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	src-1/authzone.c	src-1/authzone.c
Line	1019	1019
Object	sigsz	sigsz

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
1019.               - sigsz);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=331
Status	New

The function len in src-1/servconf.c at line 1278 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	src-1/servconf.c	src-1/servconf.c
Line	2262	2262
Object	len	len

Code Snippet
File Name src-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2262.                    options->adm_forced_command = xstrdup(str +
len);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=332
Status	New

The function len in src-1/servconf.c at line 1278 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	src-1/servconf.c	src-1/servconf.c
Line	2337	2337
Object	len	len

Code Snippet
File Name src-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2337.                        options->version_addendum = xstrdup(str +
len);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=333
Status	New

The function len in src-1/servconf.c at line 1278 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	src-1/servconf.c	src-1/servconf.c
Line	2351	2351
Object	len	len

Code Snippet
File Name src-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2351.                   *charptr = xstrdup(str + len);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=334
Status	New

The function i in src-1/session.c at line 281 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	src-1/session.c	src-1/session.c
Line	290	290
Object	i	i

Code Snippet
File Name src-1/session.c
Method set_fwdpermit_from_authopts(struct ssh *ssh, const struct sshauthopt *opts)

```
....
290.                    tmp = cp = xstrdup(auth_opts->permitopen[i]);
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=335
Status	New

The function i in src-1/session.c at line 281 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	src-1/session.c	src-1/session.c
Line	305	305
Object	i	i

Code Snippet
File Name src-1/session.c
Method set_fwdpermit_from_authopts(struct ssh *ssh, const struct sshauthopt *opts)

```
....
305.                    tmp = cp = xstrdup(auth_opts->permitlisten[i]);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=336
Status	New

The function n in src-1/session.c at line 833 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	src-1/session.c	src-1/session.c
Line	890	890
Object	n	n

Code Snippet
File Name src-1/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
890.                    ocp = xstrdup(auth_opts->env[n]);
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=337
Status	New

The function frag_len in src-1/d1_both.c at line 172 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	src-1/d1_both.c	src-1/d1_both.c
Line	187	187
Object	frag_len	frag_len

Code Snippet
File Name src-1/d1_both.c
Method dtls1_hm_fragment_new(unsigned long frag_len, int reassembly)

```
....
187.                    RSMBLY_BITMASK_SIZE(frag_len))) == NULL)
```

Wrong Size t Allocation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=338
Status	New

The function sigs in src-1/authzone.c at line 936 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	src-1/authzone.c	src-1/authzone.c
Line	955	955
Object	sigs	sigs

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
955.                + sigs*(sizeof(size_t) + sizeof(uint8_t*) +
sizeof(time_t))
```

Wrong Size t Allocation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=339
Status	New

The function sigs in src-1/authzone.c at line 936 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	src-1/authzone.c	src-1/authzone.c
Line	1018	1018
Object	sigs	sigs

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
1018.              - sigs*(sizeof(size_t) + sizeof(uint8_t*) +
sizeof(time_t))
```

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=1050100&projectid=50090&pathid=1663
Status	New

	Source	Destination
File	src-1/opts.c	src-1/opts.c
Line	96	489
Object	no_unit_at_a_time_default	no_unit_at_a_time_default

Code Snippet
File Name src-1/opts.c
Method bool no_unit_at_a_time_default;

```
....
96.  bool no_unit_at_a_time_default;
```

File Name src-1/opts.c

Method decode_options (unsigned int argc, const char **argv)

```
....
489.        if (!no_unit_at_a_time_default)
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1664
Status	New

	Source	Destination

File	src-1/drm_drv.c	src-1/drm_drv.c
Line	93	1302
Object	drm_refcnt	drm_refcnt

Code Snippet
File Name src-1/drm_drv.c
Method int drm_refcnt;

```
....
93.  int drm_refcnt;
```

File Name src-1/drm_drv.c

Method drm_attach(struct device *parent, struct device *self, void *aux)

```
....
1302.        drm_refcnt++;
```

Use of Uninitialized Variable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1665
Status New

	Source	Destination
File	src-1/drm_drv.c	src-1/drm_drv.c
Line	93	1297
Object	drm_refcnt	drm_refcnt

Code Snippet
File Name src-1/drm_drv.c
Method int drm_refcnt;

```
....
93.  int drm_refcnt;
```

File Name src-1/drm_drv.c

Method drm_attach(struct device *parent, struct device *self, void *aux)

```
....
1297.        if (drm_refcnt == 0) {
```

Use of Uninitialized Variable\Path 4:

Severity Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1666
Status	New

	Source	Destination
File	src-1/drm_drv.c	src-1/drm_drv.c
Line	93	1439
Object	drm_refcnt	drm_refcnt

Code Snippet

File Name src-1/drm_drv.c

Method int drm_refcnt;

```
....
93.  int drm_refcnt;
```

File Name src-1/drm_drv.c

Method drm_detach(struct device *self, int flags)

```
....
1439.       drm_refcnt--;
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1667
Status	New

	Source	Destination
File	src-1/drm_drv.c	src-1/drm_drv.c
Line	93	1440
Object	drm_refcnt	drm_refcnt

Code Snippet

File Name src-1/drm_drv.c

Method int drm_refcnt;

```
....
93.  int drm_refcnt;
```

File Name src-1/drm_drv.c

Method	drm_detach(struct device *self, int flags)

```
....
1440.        if (drm_refcnt == 0) {
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1668
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	88	1471
Object	crmod	crmod

Code Snippet

File Name src-1/telnet.c

Method crmod,

```
....
88.    crmod,
```

File Name src-1/telnet.c

Method telrcv(void)

```
....
1471.                    if (crmod) {
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1669
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	88	1440
Object	crmod	crmod

Code Snippet

File Name src-1/telnet.c

Method crmod,

```
....
88.    crmod,
```

File Name src-1/telnet.c

Method telrcv(void)

```
....
1440.            else if ((c == '\n') &&
my_want_state_is_dont(TELOPT_ECHO) && !crmod) {
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1670
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	88	1478
Object	crmod	crmod

Code Snippet

File Name src-1/telnet.c

Method crmod,

```
....
88.    crmod,
```

File Name src-1/telnet.c

Method telrcv(void)

```
....
1478.                if (crmod) {
```

Use of Uninitialized Variable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1671
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	90	1750
Object	crlf	crlf

Code Snippet
File Name src-1/telnet.c
Method crlf, /* Should '\r' be mapped to <CR><LF> (or <CR><NUL>)? */

```
....
90.   crlf,       /* Should '\r' be mapped to <CR><LF> (or <CR><NUL>)?
*/
```

File Name src-1/telnet.c
Method telsnd(void)

```
....
1750.             if (!crlf) {
```

Use of Uninitialized Variable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1672
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	91	1849
Object	telnetport	telnetport

Code Snippet
File Name src-1/telnet.c
Method telnetport,

```
....
91.   telnetport,
```

File Name src-1/telnet.c
Method telnet(char *user)

```
....
1849.      if (telnetport) {
```

Use of Uninitialized Variable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1673
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	95	2083
Object	autosynch	autosynch

Code Snippet

File Name src-1/telnet.c

Method autosynch, /* send interrupt characters with SYNCH? */

```
....
95.    autosynch,  /* send interrupt characters with SYNCH? */
```

File Name src-1/telnet.c

Method sendbrk(void)

```
....
2083.       if (autosynch) {
```

Use of Uninitialized Variable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1674
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	95	2069
Object	autosynch	autosynch

Code Snippet

File Name src-1/telnet.c

Method autosynch, /* send interrupt characters with SYNCH? */

```
....
95.    autosynch,  /* send interrupt characters with SYNCH? */
```

File Name src-1/telnet.c

Method intp(void)

```
....
2069.       if (autosynch) {
```

Use of Uninitialized Variable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1675
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	95	2097
Object	autosynch	autosynch

Code Snippet
File Name src-1/telnet.c
Method autosynch, /* send interrupt characters with SYNCH? */

```
....
95.    autosynch,   /* send interrupt characters with SYNCH? */
```

File Name src-1/telnet.c

Method sendabort(void)

```
....
2097.       if (autosynch) {
```

Use of Uninitialized Variable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1676
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	95	2111
Object	autosynch	autosynch

Code Snippet
File Name src-1/telnet.c
Method autosynch, /* send interrupt characters with SYNCH? */

```
....
95.   autosynch,  /* send interrupt characters with SYNCH? */
```

File Name src-1/telnet.c

Method sendsusp(void)

```
....
2111.       if (autosynch) {
```

Use of Uninitialized Variable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1677
Status New

	Source	Destination
File	src-1/rt2860.c	src-1/rt2860.c
Line	2754	2789
Object	bbp55_pb	bbp55_pb

Code Snippet
File Name src-1/rt2860.c
Method rt3090_filter_calib(struct rt2860_softc *sc, uint8_t init, uint8_t target,

```
....
2754.       uint8_t bbp55_pb, bbp55_sb, delta;
....
2789.             delta = bbp55_pb - bbp55_sb;
```

Use of Uninitialized Variable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1678
Status New

	Source	Destination
File	src-1/tmux.c	src-1/tmux.c
Line	286	290

Object	pwd	pwd

Code Snippet
File Name src-1/tmux.c
Method find_cwd(void)

```
....
286.        const char  *pwd;
....
290.        if ((pwd = getenv("PWD")) == NULL || *pwd == '\0')
```

Use of Uninitialized Variable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1679
Status New

	Source	Destination
File	src-1/zs.c	src-1/zs.c
Line	551	647
Object	rate0	rate0

Code Snippet
File Name src-1/zs.c
Method zs_set_speed(struct zs_chanstate *cs, int bps)

```
....
551.        int src, rate0, rate1, err, tol;
....
647.        bps = rate0;
```

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=1050100&projectid=50090&pathid=344
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of src-1/buf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	284	284
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/buf.c
Method translit_text(char *s, int len, int from, int to)

```
....
284.        ctab[i] = i;                    /* restore table to initial
state */
```

Char Overflow\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=345
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 278 of src-1/buf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	285	285
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/buf.c
Method translit_text(char *s, int len, int from, int to)

```
....
285.        ctab[i = from] = to;
```

Char Overflow\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=346
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 257 of src-1/buf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	src-1/buf.c	src-1/buf.c
Line	272	272
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/buf.c
Method init_buffers(void)

```
....
272.                ctab[i] = i;
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=347
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 390 of src-1/infokey.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	553	553
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
553.                oval = c - '0';
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=348
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 390 of src-1/infokey.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	516	516
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	src-1/infokey.c
Method	compile (FILE *fp, const char *filename, struct sect *sections)

```
....
516.            comment[clen++] = c;
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=349
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 390 of src-1/infokey.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	700	700
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	src-1/infokey.c
Method	compile (FILE *fp, const char *filename, struct sect *sections)

```
....
700.            act[alen++] = c;
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=350
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 390 of src-1/infokey.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	743	743
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	src-1/infokey.c
Method	compile (FILE *fp, const char *filename, struct sect *sections)

```
....
743.            varn[varlen++] = c;
```

Char Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=351
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 390 of src-1/infokey.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	767	767
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
767.            val[vallen++] = c;
```

Char Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=352
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 234 of src-1/lex.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	323	323
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/lex.c
Method ffelex_backslash_ (int c, ffewhereColumnNumber col)

```
....
323.              m[0] = c;
```

Char Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=353
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 234 of src-1/lex.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	342	342
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/lex.c
Method ffelex_backslash_ (int c, ffewhereColumnNumber col)

```
....
342.              m[0] = c;
```

Char Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=354
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1764 of src-1/lex.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	1983	1983
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/lex.c
Method ffelex_file_fixed (ffewhereFile wf, FILE *f)

```
....
1983.          label_string[labi++] = c;
```

Char Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=500

	90&pathid=355
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 882 of src-1/telnet.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	891	891
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/telnet.c
Method lm_mode(unsigned char *cmd, int len, int init)

```
....
891.        str_lm_mode[4] = linemode;
```

Char Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=356
Status	New

A variable of a larger data type, av, is being assigned to a smaller data type, in 390 of src-1/infokey.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	680	680
Object	av	av

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
680.                    char av = a;
```

Char Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=357
Status	New

A variable of a larger data type, ch, is being assigned to a smaller data type, in 956 of src-1/zs.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/zs.c	src-1/zs.c
Line	963	963
Object	ch	ch

Code Snippet
File Name src-1/zs.c
Method zscnputc(dev_t dev, int c)

```
....
963.              char ch = c;
```

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=1050100&projectid=50090&pathid=38
Status	New

The pointer ffi_type_void at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	125	125
Object	ffi_type_void	ffi_type_void

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static ffi_type *ffiTypeFor(Type *Ty) {

```
....
125.      case Type::VoidTyID: return &ffi_type_void;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=500

	90&pathid=39
Status	New

The pointer ffi_type_sint8 at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	128	128
Object	ffi_type_sint8	ffi_type_sint8

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static ffi_type *ffiTypeFor(Type *Ty) {

```
....
128.          case 8:  return &ffi_type_sint8;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=40
Status	New

The pointer ffi_type_sint16 at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	129	129
Object	ffi_type_sint16	ffi_type_sint16

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static ffi_type *ffiTypeFor(Type *Ty) {

```
....
129.          case 16: return &ffi_type_sint16;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=41
Status	New

The pointer ffi_type_sint32 at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	130	130
Object	ffi_type_sint32	ffi_type_sint32

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static ffi_type *ffiTypeFor(Type *Ty) {

```
....
130.          case 32: return &ffi_type_sint32;
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=42
Status	New

The pointer ffi_type_sint64 at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	131	131
Object	ffi_type_sint64	ffi_type_sint64

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static ffi_type *ffiTypeFor(Type *Ty) {

```
....
131.          case 64: return &ffi_type_sint64;
```

Buffer Overflow AddressOfLocalVarReturned\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=43
Status	New

The pointer ffi_type_float at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	134	134

Object	ffi_type_float	ffi_type_float

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static ffi_type *ffiTypeFor(Type *Ty) {

```
....
134.      case Type::FloatTyID:   return &ffi_type_float;
```

Buffer Overflow AddressOfLocalVarReturned\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=44
Status	New

The pointer ffi_type_double at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	135	135
Object	ffi_type_double	ffi_type_double

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static ffi_type *ffiTypeFor(Type *Ty) {

```
....
135.      case Type::DoubleTyID:  return &ffi_type_double;
```

Buffer Overflow AddressOfLocalVarReturned\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=45
Status	New

The pointer ffi_type_pointer at src-1/ExternalFunctions.cpp in line 123 is being used after it has been freed.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	136	136
Object	ffi_type_pointer	ffi_type_pointer

Code Snippet
File Name src-1/ExternalFunctions.cpp

Method	static ffi_type *ffiTypeFor(Type *Ty) {

```
....
136.      case Type::PointerTyID: return &ffi_type_pointer;
```

Buffer Overflow AddressOfLocalVarReturned\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=46
Status	New

The pointer res at src-1/replay.c in line 530 is being used after it has been freed.

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	541	541
Object	res	res

Code Snippet	
File Name	src-1/replay.c
Method	first_timer(struct replay_runtime* runtime)

```
....
541.        return res;
```

Buffer Overflow AddressOfLocalVarReturned\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=47
Status	New

The pointer d2 at src-1/tasn_enc.c in line 424 is being used after it has been freed.

	Source	Destination
File	src-1/tasn_enc.c	src-1/tasn_enc.c
Line	433	433
Object	d2	d2

Code Snippet	
File Name	src-1/tasn_enc.c
Method	der_cmp(const void *a, const void *b)

```
....
433.        return d1->length - d2->length;
```

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=1050100&projectid=50090&pathid=649
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	1015	1018
Object	cp	cp

Code Snippet
File Name src-1/channels.c
Method channel_open_message(struct ssh *ssh)

```
....
1015.                           free(cp);
....
1018.                       free(cp);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=650
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	711	711
Object	ckv	ckv

Code Snippet
File Name src-1/relayd.c
Method kv_delete(struct kvtree *keys, struct kv *kv)

```
....
711.                free(ckv);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=651
Status	New

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	2172	2172
Object	arg	arg

Code Snippet
File Name src-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2172.                    free(arg);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=652
Status	New

	Source	Destination
File	src-1/vfs_syscalls.c	src-1/vfs_syscalls.c
Line	905	910
Object	cwdbuf	cwdbuf

Code Snippet
File Name src-1/vfs_syscalls.c
Method sys___realpath(struct proc *p, void *v, register_t *retval)

```
....
905.                    free(cwdbuf, M_TEMP, cwdlen);
....
910.                    free(cwdbuf, M_TEMP, cwdlen);
```

Double Free\Path 5:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=653
Status	New

	Source	Destination
File	src-1/vfs_syscalls.c	src-1/vfs_syscalls.c
Line	905	910
Object	cwdlen	cwdlen

Code Snippet
File Name src-1/vfs_syscalls.c
Method sys___realpath(struct proc *p, void *v, register_t *retval)

```
....
905.                    free(cwdbuf, M_TEMP, cwdlen);
....
910.                    free(cwdbuf, M_TEMP, cwdlen);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=654
Status	New

	Source	Destination
File	src-1/vfs_syscalls.c	src-1/vfs_syscalls.c
Line	905	915
Object	cwdbuf	cwdbuf

Code Snippet
File Name src-1/vfs_syscalls.c
Method sys___realpath(struct proc *p, void *v, register_t *retval)

```
....
905.                    free(cwdbuf, M_TEMP, cwdlen);
....
915.                free(cwdbuf, M_TEMP, cwdlen);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=655
Status	New

	Source	Destination
File	src-1/vfs_syscalls.c	src-1/vfs_syscalls.c
Line	910	915
Object	cwdbuf	cwdbuf

Code Snippet
File Name src-1/vfs_syscalls.c
Method sys___realpath(struct proc *p, void *v, register_t *retval)

```
....
910.                    free(cwdbuf, M_TEMP, cwdlen);
....
915.            free(cwdbuf, M_TEMP, cwdlen);
```

Double Free\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=656
Status New

	Source	Destination
File	src-1/vfs_syscalls.c	src-1/vfs_syscalls.c
Line	905	915
Object	cwdlen	cwdlen

Code Snippet
File Name src-1/vfs_syscalls.c
Method sys___realpath(struct proc *p, void *v, register_t *retval)

```
....
905.                    free(cwdbuf, M_TEMP, cwdlen);
....
915.            free(cwdbuf, M_TEMP, cwdlen);
```

Double Free\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=657
Status New

	Source	Destination
File	src-1/vfs_syscalls.c	src-1/vfs_syscalls.c
Line	910	915

Object	cwdlen	cwdlen

Code Snippet
File Name src-1/vfs_syscalls.c
Method sys___realpath(struct proc *p, void *v, register_t *retval)

```
....
910.                    free(cwdbuf, M_TEMP, cwdlen);
....
915.              free(cwdbuf, M_TEMP, cwdlen);
```

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=1050100&projectid=50090&pathid=358
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 231 of src-1/asn1_item.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/asn1_item.c	src-1/asn1_item.c
Line	325	325
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/asn1_item.c
Method ASN1_item_sign_ctx(const ASN1_ITEM *it, X509_ALGOR *algor1, X509_ALGOR *algor2,

```
....
325.         ret = (int)buf_out_len;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=359
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 211 of src-1/d1_both.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	249	249
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/d1_both.c
Method dtls1_do_write(SSL *s, int type)

```
....
249.              curr_mtu = s->d1->mtu - BIO_wpending(SSL_get_wbio(s))
-
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=360
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 211 of src-1/d1_both.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	257	257
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/d1_both.c
Method dtls1_do_write(SSL *s, int type)

```
....
257.                  curr_mtu = s->d1->mtu - DTLS1_RT_HEADER_LENGTH -
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=361
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 113 of src-1/e_rc4_hmac_md5.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/e_rc4_hmac_md5.c	src-1/e_rc4_hmac_md5.c
Line	195	195
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/e_rc4_hmac_md5.c
Method rc4_hmac_md5_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
195.                    l = (key->md.Nl + (blocks << 3)) & 0xffffffffU;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=362
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 111 of src-1/nl.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/nl.c	src-1/nl.c
Line	226	226
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/nl.c
Method main(int argc, char *argv[])

```
....
226.        delimlen = delim1len + delim2len;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=363
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 509 of src-1/remote-st.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/remote-st.c	src-1/remote-st.c
Line	543	543

Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/remote-st.c
Method st2000_read_inferior_memory (CORE_ADDR memaddr, char *myaddr, int len)

```
....
543.        len_this_pass -= startaddr % 16;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=364
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 783 of src-1/servconf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	803	803
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/servconf.c
Method valid_rdomain(const char *name)

```
....
803.        mib[5] = (int)num;
```

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=1050100&projectid=50090&pathid=1802
Status	New

The size of the buffer used by rdata_match in rdatas, at line 340 of src-1/ixfrcreate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_spool_u16 passes to val, at line 254 of src-1/ixfrcreate.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	256	351
Object	val	rdatas

Code Snippet
File Name src-1/ixfrcreate.c
Method static int read_spool_u16(FILE* spool, uint16_t* val)

```
....
256.        if(fread(val, sizeof(*val), 1, spool) < 1)
```

File Name src-1/ixfrcreate.c

Method static int rdata_match(struct rr* rr, uint8_t* rdata, uint16_t rdlen)

```
....
351.                            domain_dname(rr->rdatas[i].domain)-
>name_size)
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1803
Status	New

The size of the buffer used by rdata_match in rdatas, at line 340 of src-1/ixfrcreate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_spool_u16 passes to val, at line 254 of src-1/ixfrcreate.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	256	359
Object	val	rdatas

Code Snippet
File Name src-1/ixfrcreate.c
Method static int read_spool_u16(FILE* spool, uint16_t* val)

```
....
256.        if(fread(val, sizeof(*val), 1, spool) < 1)
```

File Name src-1/ixfrcreate.c

Method	static int rdata_match(struct rr* rr, uint8_t* rdata, uint16_t rdlen)

```
....
359.                            rr->rdatas[i].data[0]) != 0)
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1804
Status	New

The size of the buffer used by process_spool_for_domain in dname_len, at line 776 of src-1/ixfrcreate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_spool_dname passes to Address, at line 270 of src-1/ixfrcreate.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	274	791
Object	Address	dname_len

Code Snippet

File Name	src-1/ixfrcreate.c
Method	static int read_spool_dname(FILE* spool, uint8_t* buf, size_t buflen,

```
....
274.        if(fread(&len, sizeof(len), 1, spool) < 1)
```

File Name	src-1/ixfrcreate.c
Method	static int process_spool_for_domain(FILE* spool, struct ixfr_create* ixfrcr,

```
....
791.                    iter->dname_len) != 0) {
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1805
Status	New

The size of the buffer used by process_spool_for_domain in dname_len, at line 776 of src-1/ixfrcreate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_spool_dname passes to buf, at line 270 of src-1/ixfrcreate.c, to overwrite the target buffer.

	Source	Destination

File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	281	791
Object	buf	dname_len

Code Snippet
File Name src-1/ixfrcreate.c
Method static int read_spool_dname(FILE* spool, uint8_t* buf, size_t buflen,

```
....
281.                if(fread(buf, len, 1, spool) < 1)
```

File Name src-1/ixfrcreate.c
Method static int process_spool_for_domain(FILE* spool, struct ixfr_create* ixfrcr,

```
....
791.                        iter->dname_len) != 0) {
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1806
Status	New

The size of the buffer used by ax_recv in sizeof, at line 98 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_recv passes to BinaryExpr, at line 98 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	115	171
Object	BinaryExpr	sizeof

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
115.                if ((nread = read(ax->ax_fd, ax->ax_rbuf + ax-
>ax_rblen,
....
171.        memcpy(&(pdu->ap_header), &header, sizeof(header));
```

Stored Buffer Overflow boundcpy\Path 6:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1807
Status	New

The size of the buffer used by ax_recv in header, at line 98 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_recv passes to BinaryExpr, at line 98 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	115	171
Object	BinaryExpr	header

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
115.              if ((nread = read(ax->ax_fd, ax->ax_rbuf + ax-
>ax_rblen,
....
171.        memcpy(&(pdu->ap_header), &header, sizeof(header));
```

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=1050100&projectid=50090&pathid=830
Status	New

The application uses a weak cryptographic algorithm, arc4random_buf at line 3922 of src-1/pf.c, to protect sensitive personal information pf_tcp_secret, from src-1/pf.c at line 3922.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	3931	3931
Object	pf_tcp_secret	arc4random_buf

Code Snippet
File Name src-1/pf.c
Method pf_tcp_iss(struct pf_pdesc *pd)

```
....
3931.            arc4random_buf(pf_tcp_secret, sizeof(pf_tcp_secret));
```

Inadequate Encryption Strength\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=831
Status	New

The application uses a weak cryptographic algorithm, arc4random_buf at line 3922 of src-1/pf.c, to protect sensitive personal information pf_tcp_secret, from src-1/pf.c at line 3922.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	3931	3931
Object	pf_tcp_secret	arc4random_buf

Code Snippet
File Name src-1/pf.c
Method pf_tcp_iss(struct pf_pdesc *pd)

```
....
3931.            arc4random_buf(pf_tcp_secret, sizeof(pf_tcp_secret));
```

Inadequate Encryption Strength\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=832
Status	New

The application uses a weak cryptographic algorithm, arc4random_buf at line 1942 of src-1/ssl_clnt.c, to protect sensitive personal information premaster_secret, from src-1/ssl_clnt.c at line 1942.

	Source	Destination
File	src-1/ssl_clnt.c	src-1/ssl_clnt.c
Line	1974	1974
Object	premaster_secret	arc4random_buf

Code Snippet
File Name src-1/ssl_clnt.c
Method ssl3_send_client_kex_gost(SSL *s, CBB *cbb)

```
....
1974.        arc4random_buf(premaster_secret, sizeof(premaster_secret));
```

Inadequate Encryption Strength\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=833
Status	New

The application uses a weak cryptographic algorithm, arc4random_buf at line 1942 of src-1/ssl_clnt.c, to protect sensitive personal information premaster_secret, from src-1/ssl_clnt.c at line 1942.

	Source	Destination
File	src-1/ssl_clnt.c	src-1/ssl_clnt.c
Line	1974	1974
Object	premaster_secret	arc4random_buf

Code Snippet
File Name src-1/ssl_clnt.c
Method ssl3_send_client_kex_gost(SSL *s, CBB *cbb)

```
....
1974.       arc4random_buf(premaster_secret, sizeof(premaster_secret));
```

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=1050100&projectid=50090&pathid=35
Status	New

The application performs an illegal operation in zs_set_speed, in src-1/zs.c. In line 547, the program attempts to divide by bps, 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 bps in zs_set_speed of src-1/zs.c, at line 547.

	Source	Destination
File	src-1/zs.c	src-1/zs.c
Line	574	574
Object	bps	bps

Code Snippet
File Name src-1/zs.c
Method zs_set_speed(struct zs_chanstate *cs, int bps)

```
....
574.                            err = abs(((rate1 - bps)*1000)/bps);
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=36
Status	New

The application performs an illegal operation in zs_set_speed, in src-1/zs.c. In line 547, the program attempts to divide by bps, 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 bps in zs_set_speed of src-1/zs.c, at line 547.

	Source	Destination
File	src-1/zs.c	src-1/zs.c
Line	613	613
Object	bps	bps

Code Snippet
File Name src-1/zs.c
Method zs_set_speed(struct zs_chanstate *cs, int bps)

```
....
613.                    err = (err * 1000)/bps;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=37
Status	New

The application performs an illegal operation in increase_dsc_bpp, in src-1/amdgpu_dm_mst_types.c. In line 737, the program attempts to divide by remaining_to_increase, 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 remaining_to_increase in increase_dsc_bpp of src-1/amdgpu_dm_mst_types.c, at line 737.

	Source	Destination
File	src-1/amdgpu_dm_mst_types.c	src-1/amdgpu_dm_mst_types.c
Line	789	789
Object	remaining_to_increase	remaining_to_increase

Code Snippet
File Name src-1/amdgpu_dm_mst_types.c
Method static int increase_dsc_bpp(struct drm_atomic_state *state,

```
....
789.                    (63 - link_timeslots_used) /
remaining_to_increase * mst_state->pbn_div;
```

Boolean Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Boolean 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

Boolean Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=341
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1094 of src-1/opts.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/opts.c	src-1/opts.c
Line	1096	1096
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/opts.c
Method set_Wextra (int setting)

```
....
1096.    extra_warnings = setting;
```

Boolean Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=342
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1111 of src-1/opts.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/opts.c	src-1/opts.c
Line	1120	1120

Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/opts.c
Method set_Wunused (int setting)

```
....
1120.    maybe_warn_unused_parameter = setting;
```

Boolean Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=343
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1156 of src-1/opts.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	src-1/opts.c	src-1/opts.c
Line	1160	1160
Object	AssignExpr	AssignExpr

Code Snippet
File Name src-1/opts.c
Method set_debug_level (enum debug_info_type type, int extended, const char *arg)

```
....
1160.    use_gnu_debug_info_extensions = extended;
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=658
Status	New

Method find_cwd at line 282 of src-1/tmux.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	src-1/tmux.c	src-1/tmux.c
Line	286	286
Object	pwd	pwd

Code Snippet
File Name src-1/tmux.c
Method find_cwd(void)

```
....
286.        const char  *pwd;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=659
Status	New

Method { at line 1130 of src-1/ipa-cp.c defines pass_ipa_cp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass_ipa_cp, this variable is never cleared from memory.

	Source	Destination
File	src-1/ipa-cp.c	src-1/ipa-cp.c
Line	1130	1130
Object	pass_ipa_cp	pass_ipa_cp

Code Snippet
File Name src-1/ipa-cp.c
Method struct tree_opt_pass pass_ipa_cp = {

```
....
1130.  struct tree_opt_pass pass_ipa_cp = {
```

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=1050100&projectid=50090&pathid=1801
Status	New

The function malloc in src-1/bytestringtest.c at line 873 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	src-1/bytestringtest.c	src-1/bytestringtest.c
Line	882	882
Object	sizeof	malloc

Code Snippet
File Name src-1/bytestringtest.c
Method test_write_bytes(void)

```
....
882.        CHECK_GOTO((tmp = malloc(sizeof(input))) != NULL);
```

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=1050100&projectid=50090&pathid=1228
Status	New

	Source	Destination
File	src-1/amdgpu_dm_mst_types.c	src-1/amdgpu_dm_mst_types.c
Line	929	929
Object	params	sizeof

Code Snippet
File Name src-1/amdgpu_dm_mst_types.c
Method static int compute_mst_dsc_configs_for_link(struct drm_atomic_state *state,

```
....
929.        memset(params, 0, sizeof(params));
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1229

Status	New

	Source	Destination
File	src-1/dce_clock_source.c	src-1/dce_clock_source.c
Line	1399	1399
Object	spread_spectrum_data	sizeof

Code Snippet
File Name src-1/dce_clock_source.c
Method static void get_ss_info_from_atombios(

```
....
1399.                    sizeof(struct spread_spectrum_data),
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1230
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	817	817
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
817.        if (NETROOM() > sizeof(str_lm)) {
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1231
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	817	817
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
817.        if (NETROOM() > sizeof(str_lm)) {
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1232
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	853	853
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
853.        if (NETROOM() > sizeof(str_lm)) {
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1233
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	853	853
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
853.        if (NETROOM() > sizeof(str_lm)) {
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1234
Status	New

	Source	Destination
File	src-1/amdgpu_dm_mst_types.c	src-1/amdgpu_dm_mst_types.c
Line	679	679
Object	dsc_cfg	sizeof

Code Snippet
File Name src-1/amdgpu_dm_mst_types.c
Method static void set_dsc_configs_from_fairness_vars(struct dsc_mst_fairness_params *params,

```
....
679.                memset(&params[i].timing->dsc_cfg, 0,
sizeof(params[i].timing->dsc_cfg));
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1235
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	766	766
Object	val	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
766.          else if (vallen < sizeof val)
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1236
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	515	515
Object	comment	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
515.          else if (clen < sizeof comment - 1)
```

Sizeof Pointer Argument\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1237
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	699	699
Object	act	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
699.          else if (alen < sizeof act - 1)
```

Sizeof Pointer Argument\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1238
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	742	742
Object	varn	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
742.          else if (varlen < sizeof varn)
```

Sizeof Pointer Argument\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1239
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	818	818
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
818.              ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1240
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	817	818
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
817.          if (NETROOM() > sizeof(str_lm)) {
818.              ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1241
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	818	818
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
818.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1242
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	817	818
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
817.        if (NETROOM() > sizeof(str_lm)) {
818.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1243
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	854	854
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
854.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1244
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	853	854
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
853.        if (NETROOM() > sizeof(str_lm)) {
854.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1245
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	854	854
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
854.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1246
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	853	854
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
853.        if (NETROOM() > sizeof(str_lm)) {
854.            ring_supply_data(&netoring, str_lm, sizeof(str_lm));
```

Sizeof Pointer Argument\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1247
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	819	819
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
819.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1248
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	817	819
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
817.        if (NETROOM() > sizeof(str_lm)) {
....
819.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1249
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	819	819
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
819.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1250
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	817	819
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_will(unsigned char *cmd, int len)

```
....
817.        if (NETROOM() > sizeof(str_lm)) {
....
819.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1251
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	855	855
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
855.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1252
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	853	855
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
853.        if (NETROOM() > sizeof(str_lm)) {
....
855.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1253
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	855	855
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
855.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1254
Status New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	853	855
Object	str_lm	sizeof

Code Snippet
File Name src-1/telnet.c
Method lm_do(unsigned char *cmd, int len)

```
....
853.        if (NETROOM() > sizeof(str_lm)) {
....
855.            printsub('>', &str_lm[2], sizeof(str_lm)-2);
```

Sizeof Pointer Argument\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1255
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	623	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
623.              To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1256
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	557	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
557.                To_seq ('\b');
....
623.              To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1257
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	561	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
561.                To_seq ('\033');
....
623.              To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1258
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	565	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
565.                To_seq ('\n');
....
623.              To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1259

Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	569	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
569.                To_seq ('\r');
....
623.              To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1260
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	573	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
573.                To_seq ('\t');
....
623.              To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1261
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c

Line	586	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
586.                  To_seq (c);
....
623.               To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1262
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	611	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
611.                   To_seq (oval);
....
623.               To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1263
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	544	623
Object	seq	sizeof

Code Snippet

File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
544.                To_seq (c);
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1264
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	642	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
642.                To_seq (CONTROL (c));
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1265
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	626	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
626.                case 'u': To_seq (SK_UP_ARROW); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1266
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	627	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
627.                case 'd': To_seq (SK_DOWN_ARROW); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1267
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	628	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
628.                case 'r': To_seq (SK_RIGHT_ARROW); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1268
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	629	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
629.                case 'l': To_seq (SK_LEFT_ARROW); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1269
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	630	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
630.                case 'U': To_seq (SK_PAGE_UP); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=500

	90&pathid=1270
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	631	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
631.                case 'D': To_seq (SK_PAGE_DOWN); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1271
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	632	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
632.                case 'h': To_seq (SK_HOME); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1272
Status	New

	Source	Destination

File	src-1/infokey.c	src-1/infokey.c
Line	633	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
633.                case 'e': To_seq (SK_END); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1273
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	634	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
634.                case 'x': To_seq (SK_DELETE); break;
....
623.                To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1274
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	635	623
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
635.              default:  To_seq (SK_LITERAL); rescan = 1; break;
....
623.              To_seq (SK_ESCAPE);
```

Sizeof Pointer Argument\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1275
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	1039	1039
Object	lowner	sizeof

Code Snippet
File Name src-1/server.c
Method recvdir(opt_t opts, int mode, char *owner, char *group)

```
....
1039.                                   sizeof(lowner));
```

Sizeof Pointer Argument\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1276
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	1044	1044
Object	lgroup	sizeof

Code Snippet
File Name src-1/server.c
Method recvdir(opt_t opts, int mode, char *owner, char *group)

```
....
1044.                                   sizeof(lgroup));
```

Sizeof Pointer Argument\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1277
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	642	642
Object	seq	sizeof

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
642.              To_seq (CONTROL (c));
```

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=1050100&projectid=50090&pathid=1808
Status	New

	Source	Destination
File	src-1/maketab.c	src-1/maketab.c
Line	139	139
Object	fgets	fgets

Code Snippet
File Name src-1/maketab.c
Method int main(int argc, char *argv[])

```
....
139.        while (fgets(buf, sizeof buf, fp) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1809
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	935	935
Object	fgets	fgets

Code Snippet
File Name src-1/relayd.c
Method rule_add(struct protocol *proto, struct relay_rule *rule, const char *rulefile)

```
....
935.        while (fgets(buf, sizeof(buf), fp) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1810
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	169	169
Object	fgets	fgets

Code Snippet
File Name src-1/replay.c
Method replay_range_read(char* remain, FILE* in, const char* name,

```
....
169.        while(fgets(line, MAX_LINE_LEN-1, in)) {
```

Improper Resource Access Authorization\Path 4:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1811
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	221	221
Object	fgets	fgets

Code Snippet
File Name src-1/replay.c
Method read_file_content(FILE* in, int* lineno, struct replay_moment* mom)

```
....
221.        if(!fgets(line, MAX_LINE_LEN-1, in))
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1812
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	225	225
Object	fgets	fgets

Code Snippet
File Name src-1/replay.c
Method read_file_content(FILE* in, int* lineno, struct replay_moment* mom)

```
....
225.        while(fgets(line, MAX_LINE_LEN-1, in)) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1813
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	448	448

Object	fgets	fgets

Code Snippet
File Name src-1/replay.c
Method replay_scenario_read(FILE* in, const char* name, int* lineno)

```
....
448.        while(fgets(line, MAX_LINE_LEN-1, in)) {
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1814
Status New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	753	753
Object	fgets	fgets

Code Snippet
File Name src-1/session.c
Method do_motd(void)

```
....
753.                    while (fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1815
Status New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1054	1054
Object	fgets	fgets

Code Snippet
File Name src-1/session.c
Method do_nologin(struct passwd *pw)

```
....
1054.             while (fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1816
Status	New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	853	853
Object	fgets	fgets

Code Snippet
File Name src-1/unifdef.c
Method parseline(void)

```
....
853.              if (fgets(tline + len, MAXLINE - len, input) == NULL)
{
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1817
Status	New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	1117	1117
Object	fgets	fgets

Code Snippet
File Name src-1/unifdef.c
Method skiphash(void)

```
....
1117.       if (fgets(tline, MAXLINE, input) == NULL) {
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1818
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	468	468
Object	fgetc	fgetc

Code Snippet
File Name src-1/infokey.c
Method compile (FILE *fp, const char *filename, struct sect *sections)

```
....
468.    while (!error && (rescan || (c = fgetc (fp)) != EOF))
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1819
Status	New

	Source	Destination
File	src-1/maketab.c	src-1/maketab.c
Line	139	139
Object	buf	buf

Code Snippet
File Name src-1/maketab.c
Method int main(int argc, char *argv[])

```
....
139.        while (fgets(buf, sizeof buf, fp) != NULL) {
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1820
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c

Line	935	935
Object	buf	buf

Code Snippet
File Name src-1/relayd.c
Method rule_add(struct protocol *proto, struct relay_rule *rule, const char *rulefile)

```
....
935.        while (fgets(buf, sizeof(buf), fp) != NULL) {
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1821
Status New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	169	169
Object	line	line

Code Snippet
File Name src-1/replay.c
Method replay_range_read(char* remain, FILE* in, const char* name,

```
....
169.        while(fgets(line, MAX_LINE_LEN-1, in)) {
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1822
Status New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	221	221
Object	line	line

Code Snippet
File Name src-1/replay.c
Method read_file_content(FILE* in, int* lineno, struct replay_moment* mom)

```
....
221.        if(!fgets(line, MAX_LINE_LEN-1, in))
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1823
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	225	225
Object	line	line

Code Snippet
File Name src-1/replay.c
Method read_file_content(FILE* in, int* lineno, struct replay_moment* mom)

```
....
225.        while(fgets(line, MAX_LINE_LEN-1, in)) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1824
Status	New

	Source	Destination
File	src-1/replay.c	src-1/replay.c
Line	448	448
Object	line	line

Code Snippet
File Name src-1/replay.c
Method replay_scenario_read(FILE* in, const char* name, int* lineno)

```
....
448.        while(fgets(line, MAX_LINE_LEN-1, in)) {
```

Improper Resource Access Authorization\Path 18:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1825
Status	New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	753	753
Object	buf	buf

Code Snippet
File Name src-1/session.c
Method do_motd(void)

```
....
753.                    while (fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1826
Status	New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1054	1054
Object	buf	buf

Code Snippet
File Name src-1/session.c
Method do_nologin(struct passwd *pw)

```
....
1054.               while (fgets(buf, sizeof(buf), f))
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1827
Status	New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	853	853

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name src-1/unifdef.c
Method parseline(void)

```
....
853.              if (fgets(tline + len, MAXLINE - len, input) == NULL)
{
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1828
Status New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	1117	1117
Object	tline	tline

Code Snippet
File Name src-1/unifdef.c
Method skiphash(void)

```
....
1117.       if (fgets(tline, MAXLINE, input) == NULL) {
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1829
Status New

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	74	74
Object	sfbuf	sfbuf

Code Snippet
File Name src-1/buf.c
Method get_sbuf_line(line_t *lp)

```
....
74.   if (fread(sfbuf, sizeof(char), len, sfp) != len) {
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1830
Status	New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	256	256
Object	val	val

Code Snippet
File Name src-1/ixfrcreate.c
Method static int read_spool_u16(FILE* spool, uint16_t* val)

```
....
256.        if(fread(val, sizeof(*val), 1, spool) < 1)
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1831
Status	New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	264	264
Object	val	val

Code Snippet
File Name src-1/ixfrcreate.c
Method static int read_spool_u32(FILE* spool, uint32_t* val)

```
....
264.        if(fread(val, sizeof(*val), 1, spool) < 1)
```

Improper Resource Access Authorization\Path 25:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1832
Status	New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	274	274
Object	Address	Address

Code Snippet
File Name src-1/ixfrcreate.c
Method static int read_spool_dname(FILE* spool, uint8_t* buf, size_t buflen,

```
....
274.        if(fread(&len, sizeof(len), 1, spool) < 1)
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1833
Status	New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	281	281
Object	buf	buf

Code Snippet
File Name src-1/ixfrcreate.c
Method static int read_spool_dname(FILE* spool, uint8_t* buf, size_t buflen,

```
....
281.              if(fread(buf, len, 1, spool) < 1)
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1834
Status	New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	421	421

Object	buf	buf

Code Snippet
File Name src-1/ixfrcreate.c
Method static int process_diff_rrset(FILE* spool, struct ixfr_create* ixfrcr,

```
....
421.              if(fread(buf, rdlen, 1, spool) < 1) {
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1835
Status New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	493	493
Object	buf	buf

Code Snippet
File Name src-1/ixfrcreate.c
Method static int process_spool_delrrset(FILE* spool, struct ixfr_create* ixfrcr,

```
....
493.              if(fread(buf, rdlen, 1, spool) < 1) {
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1836
Status New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	115	115
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
115.                if ((nread = read(ax->ax_fd, ax->ax_rbuf + ax-
>ax_rblen,
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1837
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	155	155
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
155.                nread = read(ax->ax_fd, ax->ax_rbuf + ax->ax_rblen,
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1838
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2076	2076
Object	buf	buf

Code Snippet
File Name src-1/channels.c
Method channel_handle_rfd(struct ssh *ssh, Channel *c)

```
....
2076.        len = read(c->rfd, buf, sizeof(buf));
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1839
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2225	2225
Object	buf	buf

Code Snippet
File Name src-1/channels.c
Method channel_handle_efd_read(struct ssh *ssh, Channel *c)

```
....
2225.        len = read(c->efd, buf, sizeof(buf));
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1840
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2306	2306
Object	buf	buf

Code Snippet
File Name src-1/channels.c
Method read_mux(struct ssh *ssh, Channel *c, u_int need)

```
....
2306.             len = read(c->rfd, buf, MINIMUM(rlen, CHAN_RBUF));
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1841
Status	New

	Source	Destination
File	src-1/dtstream.c	src-1/dtstream.c

Line	1549	1549
Object	Address	Address

Code Snippet
File Name src-1/dtstream.c
Method void dtio_cmd_cb(int fd, short ATTR_UNUSED(bits), void* arg)

```
....
1549.       r = read(fd, &cmd, sizeof(cmd));
```

Improper Resource Access Authorization\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1842
Status New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1310	1310
Object	buf	buf

Code Snippet
File Name src-1/relayd.c
Method relay_load_fd(int fd, off_t *len)

```
....
1310.       if ((rv = pread(fd, buf, size, 0)) != size)
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1843
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	1128	1128
Object	tbuf	tbuf

Code Snippet
File Name src-1/server.c
Method recvlink(char *new, opt_t opts, int mode, off_t size)

```
....
1128.       if ((i = readlink(target, tbuf, sizeof(tbuf)-1)) != -1) {
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1844
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	178	178
Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
178.              fprintf(stderr, "received packet:\n");
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1845
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	181	181
Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
181.                    fprintf(stderr, "%02hhx ", ax->ax_rbuf[i]);
```

Improper Resource Access Authorization\Path 39:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1846
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	187	187
Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
187.                                    fprintf(stderr, "%.4s", chars);
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1847
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	188	188
Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
188.                                fprintf(stderr, "\n");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1848
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	497	497

Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_send(struct ax *ax)

```
....
497.              fprintf(stderr, "sending packet:\n");
```

Improper Resource Access Authorization\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1849
Status New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	499	499
Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_send(struct ax *ax)

```
....
499.                    fprintf(stderr, "%02hhx ", ax->ax_wbuf[i]);
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1850
Status New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	505	505
Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_send(struct ax *ax)

```
....
505.                                    fprintf(stderr, "%.4s", chars);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1851
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	506	506
Object	fprintf	fprintf

Code Snippet
File Name src-1/ax.c
Method ax_send(struct ax *ax)

```
....
506.                            fprintf(stderr, "\n");
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1852
Status	New

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	870	870
Object	fprintf	fprintf

Code Snippet
File Name src-1/d1_both.c
Method dtls1_read_failed(SSL *s, int code)

```
....
870.                fprintf(stderr, "invalid state reached %s:%d",
```

Improper Resource Access Authorization\Path 46:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1853
Status	New

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	929	929
Object	fprintf	fprintf

Code Snippet
File Name src-1/d1_both.c
Method dtls1_retransmit_buffered_messages(SSL *s)

```
....
929.                    fprintf(stderr, "dtls1_retransmit_message()
failed\n");
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1854
Status	New

	Source	Destination
File	src-1/d1_both.c	src-1/d1_both.c
Line	1016	1016
Object	fprintf	fprintf

Code Snippet
File Name src-1/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
....
1016.             fprintf(stderr, "retransmit:  message %d non-
existent\n", seq);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1855
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c

Line	879	879
Object	fprintf	fprintf

Code Snippet
File Name src-1/infokey.c
Method error_message (int error_code, const char *fmt,

```
....
879.    fprintf (stderr, "%s: ", program_name);
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1856
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	880	880
Object	fprintf	fprintf

Code Snippet
File Name src-1/infokey.c
Method error_message (int error_code, const char *fmt,

```
....
880.    fprintf (stderr, fmt, a1, a2, a3, a4);
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1857
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	882	882
Object	fprintf	fprintf

Code Snippet
File Name src-1/infokey.c
Method error_message (int error_code, const char *fmt,

```
....
882.      fprintf (stderr, " - %s", strerror (error_code));
```

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=1050100&projectid=50090&pathid=1045
Status	New

The variable declared in null at src-1/amdgpu_dm_plane.c in line 1223 is not initialized when it is used by stream at src-1/amdgpu_dm_plane.c in line 1223.

	Source	Destination
File	src-1/amdgpu_dm_plane.c	src-1/amdgpu_dm_plane.c
Line	1229	1274
Object	null	stream

Code Snippet
File Name src-1/amdgpu_dm_plane.c
Method void handle_cursor_update(struct drm_plane *plane,

```
....
1229.       struct dm_crtc_state *crtc_state = crtc ?
to_dm_crtc_state(crtc->state) : NULL;
....
1274.       if (crtc_state->stream) {
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1046
Status	New

The variable declared in null at src-1/authzone.c in line 7688 is not initialized when it is used by Pointer at src-1/authzone.c in line 1875.

	Source	Destination

File	src-1/authzone.c	src-1/authzone.c
Line	7694	1947
Object	null	Pointer

Code Snippet
File Name src-1/authzone.c
Method int auth_zone_generate_zonemd_check(struct auth_zone* z, int scheme,

```
....
7694.        *reason = NULL;
```

File Name src-1/authzone.c
Method static int auth_zone_zonemd_check_hash(struct auth_zone* z,

```
....
1947.                                    verbose(VERB_ALGO, "auth-zone %s
ZONEMD %d %d is unsupported: %s", zstr, (int)scheme, (int)hashalgo,
*reason);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1047
Status	New

The variable declared in null at src-1/authzone.c in line 1875 is not initialized when it is used by Pointer at src-1/authzone.c in line 1875.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1936	1947
Object	null	Pointer

Code Snippet
File Name src-1/authzone.c
Method static int auth_zone_zonemd_check_hash(struct auth_zone* z,

```
....
1936.             *reason = NULL;
....
1947.                                    verbose(VERB_ALGO, "auth-zone %s
ZONEMD %d %d is unsupported: %s", zstr, (int)scheme, (int)hashalgo,
*reason);
```

NULL Pointer Dereference\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1048
Status	New

The variable declared in null at src-1/authzone.c in line 7994 is not initialized when it is used by Pointer at src-1/authzone.c in line 1875.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	7998	1947
Object	null	Pointer

Code Snippet

File Name src-1/authzone.c

Method auth_zone_verify_zonemd_with_key(struct auth_zone* z, struct module_env* env,

```
....
7998.       char* reason = NULL, *why_bogus = NULL;
```

File Name src-1/authzone.c

Method static int auth_zone_zonemd_check_hash(struct auth_zone* z,

```
....
1947.                                   verbose(VERB_ALGO, "auth-zone %s
ZONEMD %d %d is unsupported: %s", zstr, (int)scheme, (int)hashalgo,
*reason);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1049
Status	New

The variable declared in null at src-1/authzone.c in line 2094 is not initialized when it is used by task_transfer at src-1/authzone.c in line 2094.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	2097	2169
Object	null	task_transfer

Code Snippet

File Name src-1/authzone.c

Method auth_zones_cfg(struct auth_zones* az, struct config_auth* c)

```
....
2097.       struct auth_xfer* x = NULL;
....
2169.             if(!xfer_set_masters(&x->task_transfer->masters, c,
1)) {
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1050
Status	New

The variable declared in null at src-1/authzone.c in line 2094 is not initialized when it is used by task_probe at src-1/authzone.c in line 2094.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	2097	2164
Object	null	task_probe

Code Snippet
File Name src-1/authzone.c
Method auth_zones_cfg(struct auth_zones* az, struct config_auth* c)

```
....
2097.       struct auth_xfer* x = NULL;
....
2164.             if(!xfer_set_masters(&x->task_probe->masters, c, 0)) {
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1051
Status	New

The variable declared in null at src-1/authzone.c in line 3557 is not initialized when it is used by rep at src-1/authzone.c in line 3514.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3561	3526
Object	null	rep

Code Snippet

File Name src-1/authzone.c
Method int auth_zones_answer(struct auth_zones* az, struct module_env* env,

```
....
3561.       struct dns_msg* msg = NULL;
```

File Name src-1/authzone.c

Method auth_answer_encode(struct query_info* qinfo, struct module_env* env,

```
....
3526.             (int)FLAGS_GET_RCODE(msg->rep->flags), edns, repinfo,
temp, env->now_tv)
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1052
Status	New

The variable declared in null at src-1/authzone.c in line 3965 is not initialized when it is used by task_probe at src-1/authzone.c in line 6311.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3967	6317
Object	null	task_probe

Code Snippet
File Name src-1/authzone.c
Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3967.       struct auth_master* list = NULL, *last = NULL;
```

File Name src-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6317.       comm_point_delete(xfr->task_probe->cp);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=500

	90&pathid=1053
Status	New

The variable declared in null at src-1/authzone.c in line 3965 is not initialized when it is used by task_probe at src-1/authzone.c in line 6311.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3967	6314
Object	null	task_probe

Code Snippet

File Name src-1/authzone.c

Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3967.       struct auth_master* list = NULL, *last = NULL;
```

File Name src-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6314.       comm_timer_delete(xfr->task_probe->timer);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1054
Status	New

The variable declared in null at src-1/authzone.c in line 3965 is not initialized when it is used by task_probe at src-1/authzone.c in line 4129.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3967	4131
Object	null	task_probe

Code Snippet

File Name src-1/authzone.c

Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3967.       struct auth_master* list = NULL, *last = NULL;
```

File Name src-1/authzone.c

Method xfr_probe_end_of_list(struct auth_xfer* xfr)

```
....
4131.       return !xfr->task_probe->scan_specific && !xfr->task_probe-
>scan_target;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1055
Status	New

The variable declared in null at src-1/authzone.c in line 3965 is not initialized when it is used by task_probe at src-1/authzone.c in line 4129.

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	3967	4131
Object	null	task_probe

Code Snippet

File Name src-1/authzone.c

Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3967.       struct auth_master* list = NULL, *last = NULL;
```

File Name src-1/authzone.c

Method xfr_probe_end_of_list(struct auth_xfer* xfr)

```
....
4131.       return !xfr->task_probe->scan_specific && !xfr->task_probe-
>scan_target;
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1056
Status	New

The variable declared in null at src-1/ax.c in line 98 is not initialized when it is used by ap_nsr at src-1/ax.c in line 98.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	104	323
Object	null	ap_nsr

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
104.        struct ax_pdu_searchrangelist *srl = NULL;
....
323.                    srl->ap_nsr++;
```

NULL Pointer Dereference\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1057
Status New

The variable declared in null at src-1/cachedump.c in line 820 is not initialized when it is used by rep at src-1/cachedump.c in line 792.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	895	798
Object	null	rep

Code Snippet
File Name src-1/cachedump.c
Method int print_deleg_lookup(RES* ssl, struct worker* worker, uint8_t* nm,

```
....
895.                    print_dp_main(ssl, stub->dp, NULL);
```

File Name src-1/cachedump.c
Method print_dp_main(RES* ssl, struct delegpt* dp, struct dns_msg* msg)

```
....
798.            for(i=0; i<msg->rep->rrset_count; i++) {
```

NULL Pointer Dereference\Path 14:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1058
Status	New

The variable declared in null at src-1/cachedump.c in line 820 is not initialized when it is used by rep at src-1/cachedump.c in line 792.

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	846	798
Object	null	rep

Code Snippet
File Name src-1/cachedump.c
Method int print_deleg_lookup(RES* ssl, struct worker* worker, uint8_t* nm,

```
....
846.                print_dp_main(ssl, dp, NULL);
```

File Name src-1/cachedump.c
Method print_dp_main(RES* ssl, struct delegpt* dp, struct dns_msg* msg)

```
....
798.            for(i=0; i<msg->rep->rrset_count; i++) {
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1059
Status	New

The variable declared in null at src-1/cd.c in line 1196 is not initialized when it is used by port at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1215
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1215.             arg->vol[3] = audio->port[3].volume;
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1060
Status	New

The variable declared in null at src-1/cd.c in line 1196 is not initialized when it is used by port at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1214
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1214.             arg->vol[2] = audio->port[2].volume;
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1061
Status	New

The variable declared in null at src-1/cd.c in line 1196 is not initialized when it is used by port at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1213
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1213.             arg->vol[1] = audio->port[1].volume;
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1062
Status	New

The variable declared in null at src-1/cd.c in line 1196 is not initialized when it is used by port at src-1/cd.c in line 1196.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1199	1212
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_getvol(struct cd_softc *sc, struct ioc_vol *arg, int flags)

```
....
1199.       struct cd_audio_page          *audio = NULL;
....
1212.             arg->vol[0] = audio->port[0].volume;
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1063
Status	New

The variable declared in null at src-1/cd.c in line 1223 is not initialized when it is used by port at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1247
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1247.       mask_volume[3] = audio->port[3].volume;
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1064
Status	New

The variable declared in null at src-1/cd.c in line 1223 is not initialized when it is used by port at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1246
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1246.       mask_volume[2] = audio->port[2].volume;
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1065
Status	New

The variable declared in null at src-1/cd.c in line 1223 is not initialized when it is used by port at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1245
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1245.       mask_volume[1] = audio->port[1].volume;
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1066
Status	New

The variable declared in null at src-1/cd.c in line 1223 is not initialized when it is used by port at src-1/cd.c in line 1223.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1226	1244
Object	null	port

Code Snippet
File Name src-1/cd.c
Method cd_setvol(struct cd_softc *sc, const struct ioc_vol *arg, int flags)

```
....
1226.       struct cd_audio_page          *audio = NULL;
....
1244.       mask_volume[0] = audio->port[0].volume;
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1067
Status	New

The variable declared in null at src-1/cd.c in line 1299 is not initialized when it is used by flags at src-1/cd.c in line 1299.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1302	1320
Object	null	flags

Code Snippet
File Name src-1/cd.c
Method cd_set_pa_immed(struct cd_softc *sc, int flags)

```
....
1302.       struct cd_audio_page          *audio = NULL;
....
1320.             CLR(audio->flags, CD_PA_SOTC);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1068
Status	New

The variable declared in null at src-1/cd.c in line 1299 is not initialized when it is used by flags at src-1/cd.c in line 1299.

	Source	Destination
File	src-1/cd.c	src-1/cd.c
Line	1302	1321
Object	null	flags

Code Snippet
File Name src-1/cd.c
Method cd_set_pa_immed(struct cd_softc *sc, int flags)

```
....
1302.       struct cd_audio_page          *audio = NULL;
....
1321.             SET(audio->flags, CD_PA_IMMED);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1069
Status	New

The variable declared in null at src-1/channels.c in line 628 is not initialized when it is used by host_to_connect at src-1/channels.c in line 628.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	644	644
Object	null	host_to_connect

Code Snippet
File Name src-1/channels.c
Method permission_set_add(struct ssh *ssh, int who, int where,

```
....
644.        (*permp)[n].host_to_connect = MAYBE_DUP(host_to_connect);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1070
Status	New

The variable declared in null at src-1/channels.c in line 628 is not initialized when it is used by listen_host at src-1/channels.c in line 628.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	646	646
Object	null	listen_host

Code Snippet
File Name src-1/channels.c
Method permission_set_add(struct ssh *ssh, int who, int where,

```
....
646.        (*permp)[n].listen_host = MAYBE_DUP(listen_host);
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1071
Status	New

The variable declared in null at src-1/channels.c in line 628 is not initialized when it is used by listen_path at src-1/channels.c in line 628.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	647	647
Object	null	listen_path

Code Snippet
File Name src-1/channels.c
Method permission_set_add(struct ssh *ssh, int who, int where,

```
....
647.        (*permp)[n].listen_path = MAYBE_DUP(listen_path);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1072
Status	New

The variable declared in null at src-1/channels.c in line 3679 is not initialized when it is used by listening_addr at src-1/channels.c in line 3679.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	3815	3815
Object	null	listening_addr

Code Snippet
File Name src-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3815.             c->listening_addr = addr == NULL ? NULL :
xstrdup(addr);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1073
Status	New

The variable declared in 0 at src-1/channels.c in line 3679 is not initialized when it is used by listening_port at src-1/channels.c in line 3679.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	3734	3818
Object	0	listening_port

Code Snippet
File Name src-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3734.             *allocated_listen_port = 0;
....
3818.                   c->listening_port = *allocated_listen_port;
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1074
Status	New

The variable declared in null at src-1/channels.c in line 4036 is not initialized when it is used by listening_port at src-1/channels.c in line 3679.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	4044	3818
Object	null	listening_port

Code Snippet

File Name src-1/channels.c

Method channel_setup_local_fwd_listener(struct ssh *ssh,

```
....
4044.                 SSH_CHANNEL_PORT_LISTENER, fwd, NULL, fwd_opts);
```

File Name src-1/channels.c

Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3818.                   c->listening_port = *allocated_listen_port;
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1075
Status	New

The variable declared in null at src-1/drm_file.c in line 602 is not initialized when it is used by event at src-1/drm_file.c in line 630.

	Source	Destination
File	src-1/drm_file.c	src-1/drm_file.c

Line	602	630
Object	null	event

Code Snippet
File Name src-1/drm_file.c
Method struct drm_pending_event *e = NULL;

```
....
602.              struct drm_pending_event *e = NULL;
```

File Name src-1/drm_file.c

Method unsigned length = e->event->length;

```
....
630.                    unsigned length = e->event->length;
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1076
Status	New

The variable declared in null at src-1/i686_mem.c in line 424 is not initialized when it is used by mr_owner at src-1/i686_mem.c in line 424.

	Source	Destination
File	src-1/i686_mem.c	src-1/i686_mem.c
Line	438	472
Object	null	mr_owner

Code Snippet
File Name src-1/i686_mem.c
Method mrsetvariable(struct mem_range_softc *sc, struct mem_range_desc *mrd, int *arg)

```
....
438.        free_md = NULL;
....
472.        bcopy(mrd->mr_owner, free_md->mr_owner, sizeof(mrd-
>mr_owner));
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=500

	90&pathid=1077
Status	New

The variable declared in null at src-1/i915_gpu_error.c in line 851 is not initialized when it is used by context at src-1/i915_gpu_error.c in line 851.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	882	883
Object	null	context

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void __err_print_to_sgl(struct drm_i915_error_state_buf *m,

```
....
882.         for (ee = error->gt ? error->gt->engine : NULL; ee; ee = ee-
>next)
883.                 err_printf(m, "Active process (on ring %s): %s
[%d]\n",
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1078
Status	New

The variable declared in null at src-1/i915_gpu_error.c in line 851 is not initialized when it is used by context at src-1/i915_gpu_error.c in line 851.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	882	883
Object	null	context

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void __err_print_to_sgl(struct drm_i915_error_state_buf *m,

```
....
882.         for (ee = error->gt ? error->gt->engine : NULL; ee; ee = ee-
>next)
883.                 err_printf(m, "Active process (on ring %s): %s
[%d]\n",
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1079
Status	New

The variable declared in null at src-1/i915_gpu_error.c in line 851 is not initialized when it is used by engine at src-1/i915_gpu_error.c in line 851.

	Source	Destination
File	src-1/i915_gpu_error.c	src-1/i915_gpu_error.c
Line	882	883
Object	null	engine

Code Snippet
File Name src-1/i915_gpu_error.c
Method static void __err_print_to_sgl(struct drm_i915_error_state_buf *m,

```
....
882.         for (ee = error->gt ? error->gt->engine : NULL; ee; ee = ee->next)
883.                 err_printf(m, "Active process (on ring %s): %s [%d]\n",
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1080
Status	New

The variable declared in null at src-1/packet.c in line 232 is not initialized when it is used by dst at src-1/packet.c in line 232.

	Source	Destination
File	src-1/packet.c	src-1/packet.c
Line	234	248
Object	null	dst

Code Snippet
File Name src-1/packet.c
Method find_iface(struct ripd_conf *xconf, unsigned int ifindex, struct in_addr src)

```
....
234.         struct iface      *iface = NULL;
....
248.                 if (iface->dst.s_addr && iface->dst.s_addr == src.s_addr)
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1081
Status	New

The variable declared in null at src-1/packet.c in line 232 is not initialized when it is used by dst at src-1/packet.c in line 232.

	Source	Destination
File	src-1/packet.c	src-1/packet.c
Line	234	248
Object	null	dst

Code Snippet
File Name src-1/packet.c
Method find_iface(struct ripd_conf *xconf, unsigned int ifindex, struct in_addr src)

```
....
234.        struct iface      *iface = NULL;
....
248.              if (iface->dst.s_addr && iface->dst.s_addr ==
src.s_addr)
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1082
Status	New

The variable declared in null at src-1/packet.c in line 232 is not initialized when it is used by addr at src-1/packet.c in line 232.

	Source	Destination
File	src-1/packet.c	src-1/packet.c
Line	234	244
Object	null	addr

Code Snippet
File Name src-1/packet.c
Method find_iface(struct ripd_conf *xconf, unsigned int ifindex, struct in_addr src)

```
....
234.        struct iface      *iface = NULL;
....
244.              if ((iface->addr.s_addr & iface->mask.s_addr) ==
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1083
Status	New

The variable declared in null at src-1/packet.c in line 232 is not initialized when it is used by mask at src-1/packet.c in line 232.

	Source	Destination
File	src-1/packet.c	src-1/packet.c
Line	234	244
Object	null	mask

Code Snippet
File Name src-1/packet.c
Method find_iface(struct ripd_conf *xconf, unsigned int ifindex, struct in_addr src)

```
....
234.        struct iface      *iface = NULL;
....
244.              if ((iface->addr.s_addr & iface->mask.s_addr) ==
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1084
Status	New

The variable declared in null at src-1/packet.c in line 232 is not initialized when it is used by mask at src-1/packet.c in line 232.

	Source	Destination
File	src-1/packet.c	src-1/packet.c
Line	234	245
Object	null	mask

Code Snippet
File Name src-1/packet.c
Method find_iface(struct ripd_conf *xconf, unsigned int ifindex, struct in_addr src)

```
....
234.        struct iface      *iface = NULL;
....
245.                    (src.s_addr & iface->mask.s_addr))
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1085
Status	New

The variable declared in null at src-1/packet.c in line 232 is not initialized when it is used by passive at src-1/packet.c in line 232.

	Source	Destination
File	src-1/packet.c	src-1/packet.c
Line	234	241
Object	null	passive

Code Snippet
File Name src-1/packet.c
Method find_iface(struct ripd_conf *xconf, unsigned int ifindex, struct in_addr src)

```
....
234.        struct iface      *iface = NULL;
....
241.              if (iface->passive)
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1086
Status	New

The variable declared in null at src-1/pf.c in line 733 is not initialized when it is used by src at src-1/pf.c in line 1692.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	737	1699
Object	null	src

Code Snippet
File Name src-1/pf.c
Method pf_state_key_attach(struct pf_state_key *sk, struct pf_state *st, int idx)

```
....
737.        struct pf_state         *oldst = NULL;
```

File Name	src-1/pf.c
Method	pf_src_tree_remove_state(struct pf_state *st)

```
....
1699.              if (st->src.tcp_est)
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1087
Status	New

The variable declared in null at src-1/pf.c in line 1121 is not initialized when it is used by rule at src-1/pf.c in line 1121.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1126	1203
Object	null	rule

Code Snippet

File Name	src-1/pf.c
Method	pf_find_state(struct pf_pdesc *pd, struct pf_state_key_cmp *key,

```
....
1126.       struct pf_state          *st = NULL;
....
1203.              if (pf_check_threshold(&st->rule.ptr->pktrate))
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1088
Status	New

The variable declared in null at src-1/pf.c in line 1121 is not initialized when it is used by rule at src-1/pf.c in line 1121.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1126	1202
Object	null	rule

Code Snippet

File Name	src-1/pf.c
Method	pf_find_state(struct pf_pdesc *pd, struct pf_state_key_cmp *key,

```
....
1126.       struct pf_state         *st = NULL;
....
1202.             pf_add_threshold(&st->rule.ptr->pktrate);
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1089
Status	New

The variable declared in null at src-1/pf.c in line 1121 is not initialized when it is used by rule at src-1/pf.c in line 1121.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1126	1201
Object	null	rule

Code Snippet

File Name	src-1/pf.c
Method	pf_find_state(struct pf_pdesc *pd, struct pf_state_key_cmp *key,

```
....
1126.       struct pf_state         *st = NULL;
....
1201.       if (st->rule.ptr->pktrate.limit && pd->dir == st->direction)
{
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1090
Status	New

The variable declared in null at src-1/pf.c in line 1363 is not initialized when it is used by states_cur at src-1/pf.c in line 1363.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1367	1543
Object	null	states_cur

Code Snippet
File Name src-1/pf.c
Method pf_state_import(const struct pfsync_state *sp, int flags)

```
....
1367.       struct pf_rule *r = NULL;
....
1543.             r->states_cur--;
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1091
Status	New

The variable declared in null at src-1/pf.c in line 1363 is not initialized when it is used by states_tot at src-1/pf.c in line 1363.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1367	1530
Object	null	states_tot

Code Snippet
File Name src-1/pf.c
Method pf_state_import(const struct pfsync_state *sp, int flags)

```
....
1367.       struct pf_rule *r = NULL;
....
1530.       r->states_tot++;
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1092
Status	New

The variable declared in null at src-1/pf.c in line 1363 is not initialized when it is used by states_cur at src-1/pf.c in line 1363.

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	1367	1529
Object	null	states_cur

Code Snippet
File Name src-1/pf.c
Method pf_state_import(const struct pfsync_state *sp, int flags)

```
....
1367.       struct pf_rule *r = NULL;
....
1529.       r->states_cur++;
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1093
Status	New

The variable declared in null at src-1/print-udp.c in line 203 is not initialized when it is used by rr_dv at src-1/print-udp.c in line 203.

	Source	Destination
File	src-1/print-udp.c	src-1/print-udp.c
Line	206	278
Object	null	rr_dv

Code Snippet
File Name src-1/print-udp.c
Method rtcp_print(const u_char *hdr, const u_char *ep)

```
....
206.        struct rtcp_rr *rr = NULL;
....
278.                    (u_int32_t)ntohl(rr->rr_dv), ts, dts);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1094
Status	New

The variable declared in null at src-1/print-udp.c in line 203 is not initialized when it is used by rr_ls at src-1/print-udp.c in line 203.

	Source	Destination
File	src-1/print-udp.c	src-1/print-udp.c
Line	206	277
Object	null	rr_ls

Code Snippet	
File Name	src-1/print-udp.c
Method	rtcp_print(const u_char *hdr, const u_char *ep)

```
....
206.        struct rtcp_rr *rr = NULL;
....
277.                    (u_int32_t)ntohl(rr->rr_ls),
```

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=1050100&projectid=50090&pathid=878
Status	New

The LoadValueFromConsecutiveGPRRegisters method calls the snprintf function, at line 463 of src-1/ABISysV_arm64.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ABISysV_arm64.cpp	src-1/ABISysV_arm64.cpp
Line	497	497
Object	snprintf	snprintf

Code Snippet	
File Name	src-1/ABISysV_arm64.cpp
Method	static bool LoadValueFromConsecutiveGPRRegisters(

```
....
497.          ::snprintf(v_name, sizeof(v_name), "v%u", NSRN);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=879
Status	New

The auth_zone_generate_answer method calls the snprintf function, at line 3424 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	3454	3454
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method auth_zone_generate_answer(struct auth_zone* z, struct query_info* qinfo,

```
....
3454.             else  snprintf(nname, sizeof(nname), "NULL");
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=880
Status New

The auth_zone_generate_answer method calls the snprintf function, at line 3424 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	3458	3458
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method auth_zone_generate_answer(struct auth_zone* z, struct query_info* qinfo,

```
....
3458.             else  snprintf(cename, sizeof(cename), "NULL");
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=881
Status New

The auth_zone_generate_answer method calls the snprintf function, at line 3424 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	3461	3461
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method auth_zone_generate_answer(struct auth_zone* z, struct query_info* qinfo,

```
....
3461.             else  snprintf(rrstr, sizeof(rrstr), "NULL");
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=882
Status New

The xfr_write_after_update method calls the snprintf function, at line 5164 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	5209	5209
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method xfr_write_after_update(struct auth_xfer* xfr, struct module_env* env)

```
....
5209.       snprintf(tmpfile, sizeof(tmpfile), "%s.tmp%u", zfilename,
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=883
Status New

The xfr_transfer_lookup_host method calls the snprintf function, at line 5373 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	5410	5410
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method xfr_transfer_lookup_host(struct auth_xfer* xfr, struct module_env* env)

```
....
5410.             snprintf(buf1, sizeof(buf1), "auth zone %s: master
lookup"
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=884
Status New

The xfr_probe_lookup_host method calls the snprintf function, at line 6564 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	6603	6603
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method xfr_probe_lookup_host(struct auth_xfer* xfr, struct module_env* env)

```
....
6603.             snprintf(buf1, sizeof(buf1), "auth zone %s: master
lookup"
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=885
Status New

The auth_zone_zonemd_fail method calls the snprintf function, at line 7946 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	7957	7957
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method static void auth_zone_zonemd_fail(struct auth_zone* z, struct module_env* env,

```
....
7957.                   snprintf(res, sizeof(res), "%s: %s", reason,
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=886
Status New

The zonemd_lookup_dnskey method calls the snprintf function, at line 8349 of src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	8386	8386
Object	snprintf	snprintf

Code Snippet
File Name src-1/authzone.c
Method zonemd_lookup_dnskey(struct auth_zone* z, struct module_env* env)

```
....
8386.             snprintf(buf1, sizeof(buf1), "auth zone %s: lookup %s
"
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=887
Status New

The ax_error2string method calls the snprintf function, at line 791 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	850	850
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_error2string(enum ax_pdu_error error)

```
....
850.        snprintf(buffer, sizeof(buffer), "Unknown error: %d",
error);
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=888
Status New

The ax_pdutype2string method calls the snprintf function, at line 855 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	896	896
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_pdutype2string(enum ax_pdu_type type)

```
....
896.        snprintf(buffer, sizeof(buffer), "Unknown type: %d", type);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=889
Status New

The ax_closereason2string method calls the snprintf function, at line 901 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	919	919
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_closereason2string(enum ax_close_reason reason)

```
....
919.        snprintf(buffer, sizeof(buffer), "Unknown reason: %d",
reason);
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=890
Status New

The ax_oidrange2string method calls the snprintf function, at line 930 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	947	947
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_oidrange2string(struct ax_oid *oid, uint8_t range_subid,

```
....
947.                    snprintf(buf, sizeof(buf), "Couldn't parse
oid");
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=891
Status New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	968	968
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
968.                snprintf(buf, sizeof(buf), "%s: (int)%d",
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=892
Status New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1002	1002
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1002.                           snprintf(buf, sizeof(buf), "<too large
OID>: "
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=893
Status New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1018	1018
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1018.             snprintf(buf, sizeof(buf), "%s: <null>",
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=894
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1024	1024
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1024.             snprintf(buf, sizeof(buf), "%s: (oid)%s",
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=895
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1029	1029

Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1029.                    snprintf(buf, sizeof(buf), "%s:
(ipaddress)<invalid>",
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=896
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1035	1035
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1035.                    snprintf(buf, sizeof(buf), "%s: (ipaddress)"
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=897
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1041	1041
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1041.             snprintf(buf, sizeof(buf), "%s: (ipaddress)%s",
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=898
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1045	1045
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1045.             snprintf(buf, sizeof(buf), "%s: (counter32)%u",
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=899
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1049	1049
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c

Method	ax_varbind2string(struct ax_varbind *vb)

```
....
1049.             snprintf(buf, sizeof(buf), "%s: (gauge32)%u",
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=900
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1053	1053
Object	snprintf	snprintf

Code Snippet	
File Name	src-1/ax.c
Method	ax_varbind2string(struct ax_varbind *vb)

```
....
1053.             snprintf(buf, sizeof(buf), "%s: (timeticks)%u",
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=901
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1083	1083
Object	snprintf	snprintf

Code Snippet	
File Name	src-1/ax.c
Method	ax_varbind2string(struct ax_varbind *vb)

```
....
1083.             snprintf(buf, sizeof(buf), "%s: <noSuchObject>",
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=902
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1087	1087
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1087.             snprintf(buf, sizeof(buf), "%s: <noSuchInstance>",
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=903
Status	New

The ax_varbind2string method calls the snprintf function, at line 957 of src-1/ax.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	src-1/ax.c	src-1/ax.c
Line	1091	1091
Object	snprintf	snprintf

Code Snippet
File Name src-1/ax.c
Method ax_varbind2string(struct ax_varbind *vb)

```
....
1091.             snprintf(buf, sizeof(buf), "%s: <endOfMibView>",
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=904
Status	New

The channel_post_x11_listener method calls the snprintf function, at line 1762 of src-1/channels.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	src-1/channels.c	src-1/channels.c
Line	1794	1794
Object	snprintf	snprintf

Code Snippet
File Name src-1/channels.c
Method channel_post_x11_listener(struct ssh *ssh, Channel *c)

```
....
1794.       snprintf(buf, sizeof buf, "X11 connection from %.200s port
%d",
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=905
Status	New

The channel_setup_fwd_listener_tcpip method calls the snprintf function, at line 3679 of src-1/channels.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	src-1/channels.c	src-1/channels.c
Line	3721	3721
Object	snprintf	snprintf

Code Snippet
File Name src-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3721.       snprintf(strport, sizeof strport, "%d", fwd->listen_port);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=906
Status	New

The connect_to_helper method calls the snprintf function, at line 4549 of src-1/channels.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	src-1/channels.c	src-1/channels.c
Line	4587	4587
Object	snprintf	snprintf

Code Snippet
File Name src-1/channels.c
Method connect_to_helper(struct ssh *ssh, const char *name, int port, int socktype,

```
....
4587.             snprintf(strport, sizeof strport, "%d", port);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=907
Status	New

The x11_create_display_inet method calls the snprintf function, at line 4890 of src-1/channels.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	src-1/channels.c	src-1/channels.c
Line	4912	4912
Object	snprintf	snprintf

Code Snippet
File Name src-1/channels.c
Method x11_create_display_inet(struct ssh *ssh, int x11_display_offset,

```
....
4912.             snprintf(strport, sizeof strport, "%d", port);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=908
Status	New

The connect_local_xsocket method calls the snprintf function, at line 4980 of src-1/channels.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	src-1/channels.c	src-1/channels.c
Line	4990	4990
Object	snprintf	snprintf

Code Snippet
File Name src-1/channels.c
Method connect_local_xsocket(u_int dnr)

```
....
4990.       snprintf(addr.sun_path, sizeof addr.sun_path, _PATH_UNIX_X,
dnr);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=909
Status	New

The x11_connect_display method calls the snprintf function, at line 4999 of src-1/channels.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	src-1/channels.c	src-1/channels.c
Line	5065	5065
Object	snprintf	snprintf

Code Snippet
File Name src-1/channels.c
Method x11_connect_display(struct ssh *ssh)

```
....
5065.       snprintf(strport, sizeof strport, "%u", 6000 +
display_number);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=910
Status	New

The drm_attach_pci method calls the snprintf function, at line 1202 of src-1/drm_drv.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	src-1/drm_drv.c	src-1/drm_drv.c
Line	1222	1222
Object	snprintf	snprintf

Code Snippet
File Name src-1/drm_drv.c
Method drm_attach_pci(const struct drm_driver *driver, struct pci_attach_args *pa,

```
....
1222.       snprintf(arg.busid, arg.busid_len, "pci:%04x:%02x:%02x.%1x",
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=911
Status	New

The DSA_SIG_new method calls the calloc function, at line 439 of src-1/dsa_ossl.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	src-1/dsa_ossl.c	src-1/dsa_ossl.c
Line	441	441
Object	calloc	calloc

Code Snippet
File Name src-1/dsa_ossl.c
Method DSA_SIG_new(void)

```
....
441.        return calloc(1, sizeof(DSA_SIG));
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=912
Status	New

The dt_prov_syscall_init method calls the snprintf function, at line 50 of src-1/dt_prov_syscall.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	src-1/dt_prov_syscall.c	src-1/dt_prov_syscall.c
Line	75	75
Object	snprintf	snprintf

Code Snippet
File Name src-1/dt_prov_syscall.c
Method dt_prov_syscall_init(void)

```
....
75.         snprintf(sysnb, len + 1, "sys%%%u", i);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=913
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	351	351
Object	sprintf	sprintf

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
351.        sprintf(OutputBuffer++, "%c", *FmtStr++);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=914
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	354	354
Object	sprintf	sprintf

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
354.        sprintf(OutputBuffer, "%c%c", *FmtStr, *(FmtStr+1));
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=915
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	377	377
Object	sprintf	sprintf

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
377.          sprintf(Buffer, FmtBuf,
uint32_t(Args[ArgNo++].IntVal.getZExtValue()));
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=916
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	393	393
Object	sprintf	sprintf

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
393.            sprintf(Buffer, FmtBuf,
Args[ArgNo++].IntVal.getZExtValue());
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=917
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	395	395
Object	sprintf	sprintf

Code Snippet
File Name src-1/ExternalFunctions.cpp

Method	static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
395.            sprintf(Buffer,
FmtBuf,uint32_t(Args[ArgNo++].IntVal.getZExtValue()));
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=918
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	398	398
Object	sprintf	sprintf

Code Snippet	
File Name	src-1/ExternalFunctions.cpp
Method	static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
398.          sprintf(Buffer, FmtBuf, Args[ArgNo++].DoubleVal); break;
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=919
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	400	400
Object	sprintf	sprintf

Code Snippet	
File Name	src-1/ExternalFunctions.cpp

Method	static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
400.          sprintf(Buffer, FmtBuf, (void*)GVTOP(Args[ArgNo++]));
break;
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=920
Status	New

The lle_X_sprintf method calls the sprintf function, at line 337 of src-1/ExternalFunctions.cpp. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	402	402
Object	sprintf	sprintf

Code Snippet	
File Name	src-1/ExternalFunctions.cpp
Method	static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
402.          sprintf(Buffer, FmtBuf, (char*)GVTOP(Args[ArgNo++]));
break;
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=921
Status	New

The create_ixfr_spool_name method calls the snprintf function, at line 194 of src-1/ixfrcreate.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	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	198	198
Object	snprintf	snprintf

Code Snippet

File Name	src-1/ixfrcreate.c
Method	static int create_ixfr_spool_name(struct ixfr_create* ixfrcr,

```
....
198.        snprintf(buf, sizeof(buf), "%s.spoolzone.%u", zfile,
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=922
Status	New

The ixfr_create_finishup method calls the snprintf function, at line 996 of src-1/ixfrcreate.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	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	1009	1009
Object	snprintf	snprintf

Code Snippet	
File Name	src-1/ixfrcreate.c
Method	static void ixfr_create_finishup(struct ixfr_create* ixfrcr,

```
....
1009.       snprintf(nowstr, sizeof(nowstr), "%s", ctime(&now));
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=923
Status	New

The ixfr_create_finishup method calls the snprintf function, at line 996 of src-1/ixfrcreate.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	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	1012	1012
Object	snprintf	snprintf

Code Snippet	
File Name	src-1/ixfrcreate.c

Method	static void ixfr_create_finishup(struct ixfr_create* ixfrcr,

```
....
1012.       snprintf(log_buf, sizeof(log_buf),
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=924
Status	New

The ffelex_backslash_ method calls the sprintf function, at line 234 of src-1/lex.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	src-1/lex.c	src-1/lex.c
Line	363	363
Object	sprintf	sprintf

Code Snippet	
File Name	src-1/lex.c
Method	ffelex_backslash_ (int c, ffewhereColumnNumber col)

```
....
363.              sprintf (&m[0], "%x", c);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=925
Status	New

The ffelex_prepare_eos_ method calls the sprintf function, at line 837 of src-1/lex.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	src-1/lex.c	src-1/lex.c
Line	866	866
Object	sprintf	sprintf

Code Snippet	
File Name	src-1/lex.c
Method	ffelex_prepare_eos_ ()

```
....
866.            sprintf (num, "%lu", (unsigned long) ffelex_raw_mode_);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=926
Status	New

The display method calls the snprintf function, at line 428 of src-1/ls.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	src-1/ls.c	src-1/ls.c
Line	495	495
Object	snprintf	snprintf

Code Snippet
File Name src-1/ls.c
Method display(FTSENT *p, FTSENT *list)

```
....
495.                                snprintf(nuser, sizeof nuser, "%u",
sp->st_uid);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=927
Status	New

The display method calls the snprintf function, at line 428 of src-1/ls.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	src-1/ls.c	src-1/ls.c
Line	496	496
Object	snprintf	snprintf

Code Snippet
File Name src-1/ls.c
Method display(FTSENT *p, FTSENT *list)

```
....
496.                                    snprintf(ngroup, sizeof nuser, "%u",
sp->st_gid);
```

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=1050100&projectid=50090&pathid=2052
Status	New

	Source	Destination
File	src-1/amdgpu_ctx.c	src-1/amdgpu_ctx.c
Line	735	735
Object	idx	idx

Code Snippet
File Name src-1/amdgpu_ctx.c
Method uint64_t amdgpu_ctx_add_fence(struct amdgpu_ctx *ctx,

```
....
735.        centity->fences[idx] = fence;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2053
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	2737	2737
Object	rrset_count	rrset_count

Code Snippet
File Name src-1/authzone.c
Method add_synth_cname(struct auth_zone* z, uint8_t* qname, size_t qname_len,

```
....
2737.       msg->rep->rrsets[msg->rep->rrset_count] = cname;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2054
Status	New

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	408	408
Object	packetidx	packetidx

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
408.                            ax->ax_packetids[packetidx] =
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2055
Status	New

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	284	284
Object	i	i

Code Snippet
File Name src-1/buf.c
Method translit_text(char *s, int len, int from, int to)

```
....
284.        ctab[i] = i;                    /* restore table to initial
state */
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2056
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	470	470
Object	found	found

Code Snippet
File Name src-1/channels.c
Method channel_new(struct ssh *ssh, char *ctype, int type, int rfd, int wfd, int efd,

```
....
470.        c = sc->channels[found] = xcalloc(1, sizeof(Channel));
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2057
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2450	2450
Object	SSH_CHANNEL_X11_LISTENER	SSH_CHANNEL_X11_LISTENER

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2450.       pre[SSH_CHANNEL_X11_LISTENER] =
      &channel_pre_listener;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2058
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c

Line	2451	2451
Object	SSH_CHANNEL_AUTH_SOCKET	SSH_CHANNEL_AUTH_SOCKET

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2451.       pre[SSH_CHANNEL_AUTH_SOCKET] =
      &channel_pre_listener;
```

Unchecked Array Index\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2059
Status New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2452	2452
Object	SSH_CHANNEL_CONNECTING	SSH_CHANNEL_CONNECTING

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2452.       pre[SSH_CHANNEL_CONNECTING] =       &channel_pre_connecting;
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2060
Status New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2463	2463
Object	SSH_CHANNEL_X11_LISTENER	SSH_CHANNEL_X11_LISTENER

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2463.       post[SSH_CHANNEL_X11_LISTENER] =
      &channel_post_x11_listener;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2061
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2464	2464
Object	SSH_CHANNEL_AUTH_SOCKET	SSH_CHANNEL_AUTH_SOCKET

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2464.       post[SSH_CHANNEL_AUTH_SOCKET] =
      &channel_post_auth_listener;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2062
Status	New

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	2465	2465
Object	SSH_CHANNEL_CONNECTING	SSH_CHANNEL_CONNECTING

Code Snippet
File Name src-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2465.       post[SSH_CHANNEL_CONNECTING] =
      &channel_post_connecting;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2063
Status	New

	Source	Destination
File	src-1/clock.c	src-1/clock.c
Line	477	477
Object	MC_SEC	MC_SEC

Code Snippet
File Name src-1/clock.c
Method rtcsettime(struct todr_chip_handle *handle, struct timeval *tv)

```
....
477.        rtclk[MC_SEC] = bintobcd(dt.dt_sec);
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2064
Status	New

	Source	Destination
File	src-1/clock.c	src-1/clock.c
Line	478	478
Object	MC_MIN	MC_MIN

Code Snippet
File Name src-1/clock.c
Method rtcsettime(struct todr_chip_handle *handle, struct timeval *tv)

```
....
478.        rtclk[MC_MIN] = bintobcd(dt.dt_min);
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2065
Status	New

	Source	Destination

File	src-1/clock.c	src-1/clock.c
Line	479	479
Object	MC_HOUR	MC_HOUR

Code Snippet
File Name src-1/clock.c
Method rtcsettime(struct todr_chip_handle *handle, struct timeval *tv)

```
....
479.        rtclk[MC_HOUR] = bintobcd(dt.dt_hour);
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2066
Status New

	Source	Destination
File	src-1/clock.c	src-1/clock.c
Line	480	480
Object	MC_DOW	MC_DOW

Code Snippet
File Name src-1/clock.c
Method rtcsettime(struct todr_chip_handle *handle, struct timeval *tv)

```
....
480.        rtclk[MC_DOW] = dt.dt_wday + 1;
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2067
Status New

	Source	Destination
File	src-1/clock.c	src-1/clock.c
Line	481	481
Object	MC_YEAR	MC_YEAR

Code Snippet
File Name src-1/clock.c
Method rtcsettime(struct todr_chip_handle *handle, struct timeval *tv)

```
....
481.        rtclk[MC_YEAR] = bintobcd(dt.dt_year % 100);
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2068
Status	New

	Source	Destination
File	src-1/clock.c	src-1/clock.c
Line	482	482
Object	MC_MONTH	MC_MONTH

Code Snippet
File Name src-1/clock.c
Method rtcsettime(struct todr_chip_handle *handle, struct timeval *tv)

```
....
482.        rtclk[MC_MONTH] = bintobcd(dt.dt_mon);
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2069
Status	New

	Source	Destination
File	src-1/clock.c	src-1/clock.c
Line	483	483
Object	MC_DOM	MC_DOM

Code Snippet
File Name src-1/clock.c
Method rtcsettime(struct todr_chip_handle *handle, struct timeval *tv)

```
....
483.        rtclk[MC_DOM] = bintobcd(dt.dt_day);
```

Unchecked Array Index\Path 19:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2070
Status	New

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	213	213
Object	ArgNo	ArgNo

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static bool ffiInvoke(RawFunc Fn, Function *F, ArrayRef<GenericValue> ArgVals,

```
....
213.      args[ArgNo] = ffiTypeFor(ArgTy);
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2071
Status	New

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp
Line	225	225
Object	ArgNo	ArgNo

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static bool ffiInvoke(RawFunc Fn, Function *F, ArrayRef<GenericValue> ArgVals,

```
....
225.      values[ArgNo] = ffiValueFor(ArgTy, ArgVals[ArgNo],
ArgDataPtr);
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2072
Status	New

	Source	Destination
File	src-1/ExternalFunctions.cpp	src-1/ExternalFunctions.cpp

Line	389	389
Object	Size	Size

Code Snippet
File Name src-1/ExternalFunctions.cpp
Method static GenericValue lle_X_sprintf(FunctionType *FT,

```
....
389.              FmtBuf[Size] = FmtBuf[Size-1];
```

Unchecked Array Index\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2073
Status New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	78	78
Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_init(struct module_env* env, int id)

```
....
78.    env->modinfo[id] = (void*)ipsecmod_env;
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2074
Status New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	106	106
Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_new(struct module_qstate* qstate, int id)

```
....
106.        qstate->minfo[id] = iq;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2075
Status	New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	126	126
Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_error(struct module_qstate* qstate, int id)

```
....
126.        qstate->ext_state[id] = module_error;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2076
Status	New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	171	171
Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method generate_request(struct module_qstate* qstate, int id, uint8_t* name,

```
....
171.        qstate->ext_state[id] = module_wait_subquery;
```

Unchecked Array Index\Path 26:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2077
Status	New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	394	394
Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_handle_query(struct module_qstate* qstate,

```
....
394.              qstate->ext_state[id] = module_wait_module;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2078
Status	New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	410	410
Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_handle_query(struct module_qstate* qstate,

```
....
410.              qstate->ext_state[id] = module_wait_module;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2079
Status	New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	462	462

Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_handle_query(struct module_qstate* qstate,

```
....
462.        qstate->ext_state[id] = module_finished;
```

Unchecked Array Index\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2080
Status New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	601	601
Object	id	id

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_clear(struct module_qstate* qstate, int id)

```
....
601.        qstate->minfo[id] = NULL;
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2081
Status New

	Source	Destination
File	src-1/lex.c	src-1/lex.c
Line	2016	2016
Object	labi	labi

Code Snippet
File Name src-1/lex.c
Method ffelex_file_fixed (ffewhereFile wf, FILE *f)

```
....
2016.    label_string[labi] = '\0';
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2082
Status	New

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	806	806
Object	idx	idx

Code Snippet
File Name src-1/pf.c
Method pf_state_key_attach(struct pf_state_key *sk, struct pf_state *st, int idx)

```
....
806.        st->key[idx] = pf_state_key_ref(sk); /* give a ref to state
*/
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2083
Status	New

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	7401	7401
Object	dirndx	dirndx

Code Snippet
File Name src-1/pf.c
Method pf_counters_inc(int action, struct pf_pdesc *pd, struct pf_state *st,

```
....
7401.            r->bytes[dirndx] += pd->tot_len;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2084
Status	New

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	7404	7404
Object	dirndx	dirndx

Code Snippet
File Name src-1/pf.c
Method pf_counters_inc(int action, struct pf_pdesc *pd, struct pf_state *st,

```
....
7404.                    a->bytes[dirndx] += pd->tot_len;
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2085
Status	New

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	7412	7412
Object	dirndx	dirndx

Code Snippet
File Name src-1/pf.c
Method pf_counters_inc(int action, struct pf_pdesc *pd, struct pf_state *st,

```
....
7412.                        sni->sn->bytes[dirndx] += pd->tot_len;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2086
Status	New

	Source	Destination
File	src-1/pf.c	src-1/pf.c

Line	7416	7416
Object	dirndx	dirndx

Code Snippet
File Name src-1/pf.c
Method pf_counters_inc(int action, struct pf_pdesc *pd, struct pf_state *st,

```
....
7416.                    st->bytes[dirndx] += pd->tot_len;
```

Unchecked Array Index\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2087
Status New

	Source	Destination
File	src-1/pf.c	src-1/pf.c
Line	7420	7420
Object	dirndx	dirndx

Code Snippet
File Name src-1/pf.c
Method pf_counters_inc(int action, struct pf_pdesc *pd, struct pf_state *st,

```
....
7420.                          ri->r->bytes[dirndx] += pd->tot_len;
```

Unchecked Array Index\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2088
Status New

	Source	Destination
File	src-1/pfkdump.c	src-1/pfkdump.c
Line	859	859
Object	SADB_EXT_KEY_AUTH	SADB_EXT_KEY_AUTH

Code Snippet
File Name src-1/pfkdump.c
Method pfkey_print_sa(struct sadb_msg *msg, int opts)

```
....
859.              extensions[SADB_EXT_KEY_AUTH] = NULL;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2089
Status	New

	Source	Destination
File	src-1/pfkdump.c	src-1/pfkdump.c
Line	860	860
Object	SADB_EXT_KEY_ENCRYPT	SADB_EXT_KEY_ENCRYPT

Code Snippet
File Name src-1/pfkdump.c
Method pfkey_print_sa(struct sadb_msg *msg, int opts)

```
....
860.              extensions[SADB_EXT_KEY_ENCRYPT] = NULL;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2090
Status	New

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	295	295
Object	i	i

Code Snippet
File Name src-1/print-lwres.c
Method lwres_printb64len(const char *p0)

```
....
295.          b64buf[i] = (char)0;
```

Unchecked Array Index\Path 40:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2091
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	211	211
Object	PROC_RELAY	PROC_RELAY

Code Snippet
File Name src-1/relayd.c
Method main(int argc, char *argv[])

```
....
211.        ps->ps_instances[PROC_RELAY] = env->sc_conf.prefork_relay;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2092
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	212	212
Object	PROC_CA	PROC_CA

Code Snippet
File Name src-1/relayd.c
Method main(int argc, char *argv[])

```
....
212.        ps->ps_instances[PROC_CA] = env->sc_conf.prefork_relay;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2093
Status	New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	729	729

Object	rrset_id	rrset_id

Code Snippet
File Name src-1/respip.c
Method respip_data_answer(enum respip_action action,

```
....
729.        new_rep->rrsets[rrset_id] = rp;
```

Unchecked Array Index\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2094
Status New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	1076	1076
Object	id	id

Code Snippet
File Name src-1/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1076.                   qstate->minfo[id] = rq;
```

Unchecked Array Index\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2095
Status New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	1079	1079
Object	id	id

Code Snippet
File Name src-1/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1079.                    qstate->ext_state[id] = module_finished;
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2096
Status	New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	1083	1083
Object	id	id

Code Snippet
File Name src-1/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1083.              qstate->ext_state[id] = module_wait_module;
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2097
Status	New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	1136	1136
Object	id	id

Code Snippet
File Name src-1/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1136.              qstate->ext_state[id] = next_state;
```

Unchecked Array Index\Path 47:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2098
Status	New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	1138	1138
Object	id	id

Code Snippet
File Name src-1/respip.c
Method respip_operate(struct module_qstate* qstate, enum module_ev event, int id,

```
....
1138.             qstate->ext_state[id] = module_finished;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2099
Status	New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	1246	1246
Object	id	id

Code Snippet
File Name src-1/respip.c
Method respip_clear(struct module_qstate* qstate, int id)

```
....
1246.       qstate->minfo[id] = NULL;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2100
Status	New

	Source	Destination
File	src-1/rt2860.c	src-1/rt2860.c
Line	345	345

Object	IEEE80211_MODE_11G	IEEE80211_MODE_11G

Code Snippet
File Name src-1/rt2860.c
Method rt2860_attachhook(struct device *self)

```
....
345.        ic->ic_sup_rates[IEEE80211_MODE_11G] =
ieee80211_std_rateset_11g;
```

Unchecked Array Index\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2101
Status New

	Source	Destination
File	src-1/rt2860.c	src-1/rt2860.c
Line	1715	1715
Object	cur	cur

Code Snippet
File Name src-1/rt2860.c
Method rt2860_tx(struct rt2860_softc *sc, struct mbuf *m, struct ieee80211_node *ni)

```
....
1715.       ring->data[ring->cur] = data;
```

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=1050100&projectid=50090&pathid=842
Status New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	383
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
```

Privacy Violation\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=843
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	384
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
```

Privacy Violation\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=844
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c

Line	384	415
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
415.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=845
Status New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	415
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
415.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=846
Status New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	415

Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
415.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=847
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	432
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
432.                          printf("[0x%x]", v);
```

Privacy Violation\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=848
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	432
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
432.                            printf("[0x%x]", v);
```

Privacy Violation\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=849
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	432
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
432.                            printf("[0x%x]", v);
```

Privacy Violation\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=850
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	445
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
445.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=851
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	445
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
445.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=852
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	445
Object	authtype	printf

Code Snippet

File Name	src-1/print-lwres.c
Method	lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
445.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=853
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	487
Object	authlength	printf

Code Snippet

File Name	src-1/print-lwres.c
Method	lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
487.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=854
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	487
Object	authlength	printf

Code Snippet

File Name	src-1/print-lwres.c

Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
487.                            printf(" flags:0x%lx",
```

Privacy Violation\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=855
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	487
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
487.                            printf(" flags:0x%lx",
```

Privacy Violation\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=856
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	491
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
491.                    printf(" %u/%u", ntohs(gabn->naliases),
```

Privacy Violation\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=857
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	491
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
491.                    printf(" %u/%u", ntohs(gabn->naliases),
```

Privacy Violation\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=858
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	491
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
491.                    printf(" %u/%u", ntohs(gabn->naliases),
```

Privacy Violation\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=859
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	527
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
527.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=860
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	527
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
527.                            printf(" flags:0x%lx",
```

Privacy Violation\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=861
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	527
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
527.                            printf(" flags:0x%lx",
```

Privacy Violation\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=862
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	531
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
531.                    printf(" %u", ntohs(gnba->naliases));
```

Privacy Violation\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=863
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	531
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
531.                    printf(" %u", ntohs(gnba->naliases));
```

Privacy Violation\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=864
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	531
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
531.                    printf(" %u", ntohs(gnba->naliases));
```

Privacy Violation\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=865
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	554
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
554.                          printf(" flags:0x%lx",
```

Privacy Violation\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=866
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	554
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
554.                            printf(" flags:0x%lx",
```

Privacy Violation\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=867
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	554
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
554.                            printf(" flags:0x%lx",
```

Privacy Violation\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=868
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	558
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
558.                    printf(" %s", tok2str(ns_type2str, "Type%d",
```

Privacy Violation\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=869
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	558
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
558.                    printf(" %s", tok2str(ns_type2str, "Type%d",
```

Privacy Violation\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=870
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	558
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
558.                    printf(" %s", tok2str(ns_type2str, "Type%d",
```

Privacy Violation\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=871
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	561
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
561.                            printf(" %s", tok2str(ns_class2str,
"Class%d",
```

Privacy Violation\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=872
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	561
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
561.                          printf(" %s", tok2str(ns_class2str,
"Class%d",
```

Privacy Violation\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=873
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	561
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
561.                          printf(" %s", tok2str(ns_class2str,
"Class%d",
```

Privacy Violation\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=874
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	384	565
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
384.                    printf(" authlen:%u", ntohs(np->authlength));
....
565.                    printf(" %u/%u", ntohs(grbn->nrdatas),
```

Privacy Violation\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=875
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	353	565
Object	authlength	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
353.        TCHECK(np->authlength);
....
565.                    printf(" %u/%u", ntohs(grbn->nrdatas),
```

Privacy Violation\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=876
Status	New

Method lwres_print at line 343 of src-1/print-lwres.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/print-lwres.c	src-1/print-lwres.c
Line	383	565
Object	authtype	printf

Code Snippet
File Name src-1/print-lwres.c
Method lwres_print(const u_char *bp, u_int length)

```
....
383.                    printf(" authtype:0x%x", ntohs(np->authtype));
....
565.                    printf(" %u/%u", ntohs(grbn->nrdatas),
```

Privacy Violation\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=877
Status	New

Method dump_config at line 2919 of src-1/servconf.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	3033	2871
Object	auth_methods	printf

Code Snippet

File Name src-1/servconf.c

Method dump_config(ServerOptions *o)

```
....
3033.           o->num_auth_methods, o->auth_methods);
```

File Name src-1/servconf.c

Method dump_cfg_strarray_oneline(ServerOpCodes code, u_int count, char **vals)

```
....
2871.             printf(" %s",  vals[i]);
```

TOCTOU

Query Path:

CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2023
Status	New

The az_parse_file method in src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	1516	1516
Object	fopen	fopen

Code Snippet
File Name src-1/authzone.c
Method az_parse_file(struct auth_zone* z, FILE* in, uint8_t* rr, size_t rrbuflen,

```
....
1516.                           inc = fopen(incfile, "r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2024
Status	New

The auth_zone_read_zonefile method in src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	1585	1585
Object	fopen	fopen

Code Snippet
File Name src-1/authzone.c
Method auth_zone_read_zonefile(struct auth_zone* z, struct config_file* cfg)

```
....
1585.       in = fopen(zfilename, "r");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2025
Status	New

The auth_zone_write_file method in src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	1733	1733
Object	fopen	fopen

Code Snippet
File Name src-1/authzone.c
Method int auth_zone_write_file(struct auth_zone* z, const char* fname)

```
....
1733.        out = fopen(fname, "w");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2026
Status	New

The auth_zone_write_chunks method in src-1/authzone.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	src-1/authzone.c	src-1/authzone.c
Line	5146	5146
Object	fopen	fopen

Code Snippet
File Name src-1/authzone.c
Method auth_zone_write_chunks(struct auth_xfer* xfr, const char* fname)

```
....
5146.        out = fopen(fname, "w");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2027
Status	New

The main method in src-1/infokey.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	src-1/infokey.c	src-1/infokey.c

Line	203	203
Object	fopen	fopen

Code Snippet
File Name src-1/infokey.c
Method main (int argc, char **argv)

```
....
203.      inf = fopen (input_filename, "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2028
Status	New

The main method in src-1/infokey.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	src-1/infokey.c	src-1/infokey.c
Line	217	217
Object	fopen	fopen

Code Snippet
File Name src-1/infokey.c
Method main (int argc, char **argv)

```
....
217.        outf = fopen (output_filename, FOPEN_WBIN);
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2029
Status	New

The spool_zone_to_file method in src-1/ixfrcreate.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	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	165	165
Object	fopen	fopen

Code Snippet	
File Name	src-1/ixfrcreate.c
Method	static int spool_zone_to_file(struct zone* zone, char* file_name,

```
....
165.        out = fopen(file_name, "w");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2030
Status	New

The ixfr_perform_init method in src-1/ixfrcreate.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	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	939	939
Object	fopen	fopen

Code Snippet	
File Name	src-1/ixfrcreate.c
Method	static int ixfr_perform_init(struct ixfr_create* ixfrcr, struct zone* zone,

```
....
939.        *spool = fopen(ixfrcr->file_name, "r");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2031
Status	New

The main method in src-1/maketab.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	src-1/maketab.c	src-1/maketab.c
Line	133	133
Object	fopen	fopen

Code Snippet	
File Name	src-1/maketab.c

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

```
....
133.        if ((fp = fopen(argv[1], "r")) == NULL) {
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2032
Status	New

The rule_add method in src-1/relayd.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	src-1/relayd.c	src-1/relayd.c
Line	932	932
Object	fopen	fopen

Code Snippet	
File Name	src-1/relayd.c
Method	rule_add(struct protocol *proto, struct relay_rule *rule, const char *rulefile)

```
....
932.        if ((fp = fopen(rulefile, "r")) == NULL)
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2033
Status	New

The st2000_open method in src-1/remote-st.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	src-1/remote-st.c	src-1/remote-st.c
Line	303	303
Object	fopen	fopen

Code Snippet	
File Name	src-1/remote-st.c
Method	st2000_open (char *args, int from_tty)

```
....
303.    log_file = fopen (LOG_FILE, "w");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2034
Status	New

The load_server_config method in src-1/servconf.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	src-1/servconf.c	src-1/servconf.c
Line	2547	2547
Object	fopen	fopen

Code Snippet
File Name src-1/servconf.c
Method load_server_config(const char *filename, struct sshbuf *conf)

```
....
2547.       if ((f = fopen(filename, "r")) == NULL) {
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2035
Status	New

The recvfile method in src-1/server.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	src-1/server.c	src-1/server.c
Line	804	804
Object	fopen	fopen

Code Snippet
File Name src-1/server.c
Method recvfile(char *new, opt_t opts, int mode, char *owner, char *group,

```
....
804.              if ((f1 = fopen(target, "r")) == NULL) {
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2036
Status	New

The recvfile method in src-1/server.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	src-1/server.c	src-1/server.c
Line	811	811
Object	fopen	fopen

Code Snippet
File Name src-1/server.c
Method recvfile(char *new, opt_t opts, int mode, char *owner, char *group,

```
....
811.              if ((f2 = fopen(new, "r")) == NULL) {
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2037
Status	New

The do_motd method in src-1/session.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	750	750
Object	fopen	fopen

Code Snippet
File Name src-1/session.c
Method do_motd(void)

```
....
750.              f = fopen(login_getcapstr(lc, "welcome", "/etc/motd",
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2038
Status	New

The read_environment_file method in src-1/session.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	797	797
Object	fopen	fopen

Code Snippet
File Name src-1/session.c
Method read_environment_file(char ***env, u_int *envsize,

```
....
797.        f = fopen(filename, "r");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2039
Status	New

The do_nologin method in src-1/session.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1053	1053
Object	fopen	fopen

Code Snippet
File Name src-1/session.c
Method do_nologin(struct passwd *pw)

```
....
1053.       if ((f = fopen(nl, "r")) != NULL) {
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2040
Status	New

The processinout method in src-1/unifdef.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	src-1/unifdef.c	src-1/unifdef.c
Line	404	404
Object	fopen	fopen

Code Snippet
File Name src-1/unifdef.c
Method processinout(const char *ifn, const char *ofn)

```
....
404.              input = fopen(ifn, "rb");
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2041
Status	New

The processinout method in src-1/unifdef.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	src-1/unifdef.c	src-1/unifdef.c
Line	414	414
Object	fopen	fopen

Code Snippet
File Name src-1/unifdef.c
Method processinout(const char *ifn, const char *ofn)

```
....
414.              output = fopen(ofn, "wb");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2042
Status	New

The defundefile method in src-1/unifdef.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	src-1/unifdef.c	src-1/unifdef.c
Line	1461	1461
Object	fopen	fopen

Code Snippet
File Name src-1/unifdef.c
Method defundefile(const char *fn)

```
....
1461.       input = fopen(fn, "rb");
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2043
Status	New

The drm_stub_open method in src-1/drm_drv.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	src-1/drm_drv.c	src-1/drm_drv.c
Line	1113	1113
Object	open	open

Code Snippet
File Name src-1/drm_drv.c
Method static int drm_stub_open(struct inode *inode, struct file *filp)

```
....
1113.             err = filp->f_op->open(inode, filp);
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2044
Status	New

The *drm_file_alloc method in src-1/drm_file.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	src-1/drm_file.c	src-1/drm_file.c
Line	188	188
Object	open	open

Code Snippet
File Name src-1/drm_file.c
Method struct drm_file *drm_file_alloc(struct drm_minor *minor)

```
....
188.             ret = dev->driver->open(dev, file);
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2045
Status	New

The relay_load_certfiles method in src-1/relayd.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	src-1/relayd.c	src-1/relayd.c
Line	1339	1339
Object	open	open

Code Snippet
File Name src-1/relayd.c
Method relay_load_certfiles(struct relayd *env, struct relay *rlay, const char *name)

```
....
1339.                        open(proto->tlsca, O_RDONLY)) == -1)
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2046
Status	New

The relay_load_certfiles method in src-1/relayd.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	src-1/relayd.c	src-1/relayd.c
Line	1345	1345
Object	open	open

Code Snippet
File Name src-1/relayd.c
Method relay_load_certfiles(struct relayd *env, struct relay *rlay, const char *name)

```
....
1345.                        open(proto->tlscacert, O_RDONLY)) == -1)
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2047
Status	New

The relay_load_certfiles method in src-1/relayd.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	src-1/relayd.c	src-1/relayd.c
Line	1375	1375
Object	open	open

Code Snippet
File Name src-1/relayd.c
Method relay_load_certfiles(struct relayd *env, struct relay *rlay, const char *name)

```
....
1375.       if ((cert_fd = open(certfile, O_RDONLY)) == -1) {
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2048
Status	New

The relay_load_certfiles method in src-1/relayd.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	src-1/relayd.c	src-1/relayd.c
Line	1379	1379
Object	open	open

Code Snippet
File Name src-1/relayd.c
Method relay_load_certfiles(struct relayd *env, struct relay *rlay, const char *name)

```
....
1379.             if ((cert_fd = open(certfile, O_RDONLY)) == -1)
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2049
Status	New

The relay_load_certfiles method in src-1/relayd.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	src-1/relayd.c	src-1/relayd.c
Line	1394	1394
Object	open	open

Code Snippet
File Name src-1/relayd.c
Method relay_load_certfiles(struct relayd *env, struct relay *rlay, const char *name)

```
....
1394.       if ((key_fd = open(certfile, O_RDONLY)) == -1)
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2050
Status	New

The relay_load_certfiles method in src-1/relayd.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	src-1/relayd.c	src-1/relayd.c
Line	1407	1407
Object	open	open

Code Snippet
File Name src-1/relayd.c
Method relay_load_certfiles(struct relayd *env, struct relay *rlay, const char *name)

```
....
1407.       if ((ocsp_fd = open(certfile, O_RDONLY)) != -1)
```

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=1050100&projectid=50090&pathid=1977
Status	New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	165	165
Object	chmod	chmod

Code Snippet
File Name src-1/server.c
Method setfilemode(char *file, int fd, int mode, int islink)

```
....
165.              status = chmod(file, mode);
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1978
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	986	986
Object	chmod	chmod

Code Snippet
File Name src-1/server.c
Method recvdir(opt_t opts, int mode, char *owner, char *group)

```
....
986.                          else if (chmod(target, mode) != 0)
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1979
Status New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1516	1516
Object	inc	inc

Code Snippet
File Name src-1/authzone.c
Method az_parse_file(struct auth_zone* z, FILE* in, uint8_t* rr, size_t rrbuflen,

```
....
1516.                          inc = fopen(incfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1980
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1585	1585
Object	in	in

Code Snippet
File Name src-1/authzone.c
Method auth_zone_read_zonefile(struct auth_zone* z, struct config_file* cfg)

```
....
1585.       in = fopen(zfilename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1981
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1733	1733
Object	out	out

Code Snippet
File Name src-1/authzone.c
Method int auth_zone_write_file(struct auth_zone* z, const char* fname)

```
....
1733.       out = fopen(fname, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1982
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	5146	5146
Object	out	out

Code Snippet
File Name src-1/authzone.c
Method auth_zone_write_chunks(struct auth_xfer* xfr, const char* fname)

```
....
5146.        out = 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=1050100&projectid=50090&pathid=1983
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	203	203
Object	inf	inf

Code Snippet
File Name src-1/infokey.c
Method main (int argc, char **argv)

```
....
203.       inf = fopen (input_filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1984
Status New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	217	217
Object	outf	outf

Code Snippet

File Name	src-1/infokey.c
Method	main (int argc, char **argv)

```
....
217.        outf = fopen (output_filename, FOPEN_WBIN);
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1985
Status	New

	Source	Destination
File	src-1/ixfrcreate.c	src-1/ixfrcreate.c
Line	165	165
Object	out	out

Code Snippet

File Name	src-1/ixfrcreate.c
Method	static int spool_zone_to_file(struct zone* zone, char* file_name,

```
....
165.        out = fopen(file_name, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1986
Status	New

	Source	Destination
File	src-1/maketab.c	src-1/maketab.c
Line	133	133
Object	fp	fp

Code Snippet

File Name	src-1/maketab.c
Method	int main(int argc, char *argv[])

```
....
133.        if ((fp = fopen(argv[1], "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=1050100&projectid=50090&pathid=1987
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	932	932
Object	fp	fp

Code Snippet
File Name src-1/relayd.c
Method rule_add(struct protocol *proto, struct relay_rule *rule, const char *rulefile)

```
....
932.        if ((fp = fopen(rulefile, "r")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1988
Status	New

	Source	Destination
File	src-1/remote-st.c	src-1/remote-st.c
Line	303	303
Object	log_file	log_file

Code Snippet
File Name src-1/remote-st.c
Method st2000_open (char *args, int from_tty)

```
....
303.    log_file = fopen (LOG_FILE, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1989
Status	New

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c

Line	2547	2547
Object	f	f

Code Snippet
File Name src-1/servconf.c
Method load_server_config(const char *filename, struct sshbuf *conf)

```
....
2547.       if ((f = fopen(filename, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1990
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	804	804
Object	f1	f1

Code Snippet
File Name src-1/server.c
Method recvfile(char *new, opt_t opts, int mode, char *owner, char *group,

```
....
804.              if ((f1 = fopen(target, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1991
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	811	811
Object	f2	f2

Code Snippet
File Name src-1/server.c
Method recvfile(char *new, opt_t opts, int mode, char *owner, char *group,

```
....
811.              if ((f2 = fopen(new, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1992
Status	New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	750	750
Object	f	f

Code Snippet
File Name src-1/session.c
Method do_motd(void)

```
....
750.              f = fopen(login_getcapstr(lc, "welcome", "/etc/motd",
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1993
Status	New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	797	797
Object	f	f

Code Snippet
File Name src-1/session.c
Method read_environment_file(char ***env, u_int *envsize,

```
....
797.          f = fopen(filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1994
Status	New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1053	1053
Object	f	f

Code Snippet
File Name src-1/session.c
Method do_nologin(struct passwd *pw)

```
....
1053.       if ((f = fopen(nl, "r")) != NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1995
Status	New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	404	404
Object	input	input

Code Snippet
File Name src-1/unifdef.c
Method processinout(const char *ifn, const char *ofn)

```
....
404.              input = fopen(ifn, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1996
Status	New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	414	414

Object	output	output

Code Snippet
File Name src-1/unifdef.c
Method processinout(const char *ifn, const char *ofn)

```
....
414.              output = fopen(ofn, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1997
Status New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	1461	1461
Object	input	input

Code Snippet
File Name src-1/unifdef.c
Method defundefile(const char *fn)

```
....
1461.       input = fopen(fn, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1998
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	654	654
Object	mkdir	mkdir

Code Snippet
File Name src-1/server.c
Method chkparent(char *name, opt_t opts)

```
....
654.                    if (mkdir(name, 0777 & ~oumask) == 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1999
Status	New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	1080	1080
Object	mkdir	mkdir

Code Snippet
File Name src-1/server.c
Method recvdir(opt_t opts, int mode, char *owner, char *group)

```
....
1080.                   if (mkdir(target, mode) == 0 ||
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2000
Status	New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	1082	1082
Object	mkdir	mkdir

Code Snippet
File Name src-1/server.c
Method recvdir(opt_t opts, int mode, char *owner, char *group)

```
....
1082.                       mkdir(target, mode) == 0)) {
```

Incorrect Permission Assignment For Critical Resources\Path 25:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2001
Status	New

	Source	Destination
File	src-1/tmux.c	src-1/tmux.c
Line	215	215
Object	mkdir	mkdir

Code Snippet
File Name src-1/tmux.c
Method make_label(const char *label, char **cause)

```
....
215.        if (mkdir(base, S_IRWXU) != 0 && errno != EEXIST) {
```

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=1050100&projectid=50090&pathid=997
Status	New

	Source	Destination
File	src-1/dt_prov_syscall.c	src-1/dt_prov_syscall.c
Line	52	60
Object	dtp	sizeof

Code Snippet
File Name src-1/dt_prov_syscall.c
Method dt_prov_syscall_init(void)

```
....
52.    struct dt_probe *dtp;
....
60.    dtps_return = mallocarray(dtps_nsysent, sizeof(dtp), M_DT,
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=998
Status	New

	Source	Destination
File	src-1/dt_prov_syscall.c	src-1/dt_prov_syscall.c
Line	52	56
Object	dtp	sizeof

Code Snippet
File Name src-1/dt_prov_syscall.c
Method dt_prov_syscall_init(void)

```
....
52.   struct dt_probe *dtp;
....
56.   dtps_entry = mallocarray(dtps_nsysent, sizeof(dtp), M_DT,
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=999
Status New

	Source	Destination
File	src-1/dt_prov_syscall.c	src-1/dt_prov_syscall.c
Line	52	63
Object	dtp	sizeof

Code Snippet
File Name src-1/dt_prov_syscall.c
Method dt_prov_syscall_init(void)

```
....
52.   struct dt_probe *dtp;
....
63.         free(dtps_entry, M_DT, dtps_nsysent * sizeof(dtp));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1000
Status New

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	72	73

Object	ipsecmod_env	sizeof

Code Snippet
File Name src-1/ipsecmod.c
Method ipsecmod_init(struct module_env* env, int id)

```
....
72.   struct ipsecmod_env* ipsecmod_env = (struct
ipsecmod_env*)calloc(1,
73.          sizeof(struct ipsecmod_env));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1001
Status New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	147	147
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method msg_grow_array(struct regional* region, struct dns_msg* msg)

```
....
147.                    sizeof(struct ub_packed_rrset_key*)*(msg->rep-
>rrset_count+1));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1002
Status New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	153	153
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method msg_grow_array(struct regional* region, struct dns_msg* msg)

```
....
153.                    sizeof(struct ub_packed_rrset_key*)*(msg->rep-
>rrset_count+1));
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1003
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	157	157
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method msg_grow_array(struct regional* region, struct dns_msg* msg)

```
....
157.                    sizeof(struct ub_packed_rrset_key*)*msg->rep-
>rrset_count);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1004
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	740	740
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method rrset_remove_rr(struct auth_rrset* rrset, size_t index)

```
....
740.              sizeof(size_t) + sizeof(uint8_t*) + sizeof(time_t) +
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1005
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	802	802
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method rrset_add_rr(struct auth_rrset* rrset, uint32_t rr_ttl, uint8_t* rdata,

```
....
802.             + sizeof(size_t) + sizeof(uint8_t*) + sizeof(time_t)
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1006
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	881	881
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method rrset_create(struct auth_data* node, uint16_t rr_type, uint32_t rr_ttl,

```
....
881.             sizeof(uint8_t*) + sizeof(time_t) + rdatalen);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1007
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c

Line	955	955
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
955.                + sigs*(sizeof(size_t) + sizeof(uint8_t*) +
sizeof(time_t))
```

Use of Sizeof On a Pointer Type\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1008
Status New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1016	1016
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
1016.               sizeof(uint8_t*) + sizeof(time_t)) + sigsz);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1009
Status New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	1018	1018
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method rrset_moveover_rrsigs(struct auth_data* node, uint16_t rr_type,

```
....
1018.              - sigs*(sizeof(size_t) + sizeof(uint8_t*) +
sizeof(time_t))
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1010
Status	New

	Source	Destination
File	src-1/authzone.c	src-1/authzone.c
Line	2697	2697
Object	sizeof	sizeof

Code Snippet
File Name src-1/authzone.c
Method create_synth_cname(uint8_t* qname, size_t qname_len, struct regional* region,

```
....
2697.              sizeof(uint8_t*) + sizeof(time_t) + sizeof(uint16_t)
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1011
Status	New

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	234	234
Object	sizeof	sizeof

Code Snippet
File Name src-1/cachedump.c
Method copy_msg(struct regional* region, struct lruhash_entry* e,

```
....
234.               sizeof(struct ub_packed_rrset_key*) * rep-
>rrset_count);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1012
Status	New

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	404	404
Object	sizeof	sizeof

Code Snippet
File Name src-1/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
404.        s = sizeof(*ad) + (sizeof(size_t) + sizeof(uint8_t*) +
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1013
Status	New

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	419	419
Object	sizeof	sizeof

Code Snippet
File Name src-1/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
419.        memmove(p, &d->rr_data[0], sizeof(uint8_t*)*num);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1014
Status	New

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c

Line	420	420
Object	sizeof	sizeof

Code Snippet
File Name src-1/cachedump.c
Method move_into_cache(struct ub_packed_rrset_key* k,

```
....
420.        p += sizeof(uint8_t*)*num;
```

Use of Sizeof On a Pointer Type\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1015
Status New

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	493	493
Object	sizeof	sizeof

Code Snippet
File Name src-1/cachedump.c
Method load_rrset(RES* ssl, sldns_buffer* buf, struct worker* worker)

```
....
493.                sizeof(uint8_t*)*(d->count+d->rrsig_count));
```

Use of Sizeof On a Pointer Type\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1016
Status New

	Source	Destination
File	src-1/cachedump.c	src-1/cachedump.c
Line	669	669
Object	sizeof	sizeof

Code Snippet
File Name src-1/cachedump.c
Method load_msg(RES* ssl, sldns_buffer* buf, struct worker* worker)

```
....
669.              region, sizeof(struct
ub_packed_rrset_key*)*rep.rrset_count);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1017
Status	New

	Source	Destination
File	src-1/glob.c	src-1/glob.c
Line	577	577
Object	sizeof	sizeof

Code Snippet
File Name src-1/glob.c
Method glob0(const Char *pattern, glob_t *pglob, struct glob_lim *limitp)

```
....
577.                          pglob->gl_pathc - oldpathc, sizeof(char *),
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1018
Status	New

	Source	Destination
File	src-1/respip.c	src-1/respip.c
Line	520	520
Object	sizeof	sizeof

Code Snippet
File Name src-1/respip.c
Method respip_copy_rrset(const struct ub_packed_rrset_key* key, struct regional* region)

```
....
520.              (sizeof(size_t)+sizeof(uint8_t*)+sizeof(time_t));
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1019
Status	New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	843	843
Object	sizeof	sizeof

Code Snippet
File Name src-1/session.c
Method do_setup_env(struct ssh *ssh, Session *s, const char *shell)

```
....
843.        env = xcalloc(envsize, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1020
Status	New

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	497	497
Object	sizeof	sizeof

Code Snippet
File Name src-1/telnet.c
Method mklist(char *buf, char *name)

```
....
497.        argv = reallocarray(NULL, n+3, sizeof(char *));
```

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=1050100&projectid=50090&pathid=2002
Status	New

The system data read by *MallocIntrospectionLockForker in the file src-1/asan_mac_test.cpp at line 151 is potentially exposed by *MallocIntrospectionLockForker found in src-1/asan_mac_test.cpp at line 151.

	Source	Destination
File	src-1/asan_mac_test.cpp	src-1/asan_mac_test.cpp
Line	154	154
Object	perror	perror

Code Snippet
File Name src-1/asan_mac_test.cpp
Method void *MallocIntrospectionLockForker(void *_) {

```
....
154.      perror("fork");
```

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=1050100&projectid=50090&pathid=2003
Status	New

The system data read by get_sbuf_line in the file src-1/buf.c at line 54 is potentially exposed by get_sbuf_line found in src-1/buf.c at line 54.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	67	67
Object	perror	perror

Code Snippet
File Name src-1/buf.c
Method get_sbuf_line(line_t *lp)

```
....
67.               perror(NULL);
```

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=1050100&projectid=500

	90&pathid=2004
Status	New

The system data read by get_sbuf_line in the file src-1/buf.c at line 54 is potentially exposed by get_sbuf_line found in src-1/buf.c at line 54.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	75	75
Object	perror	perror

Code Snippet
File Name src-1/buf.c
Method get_sbuf_line(line_t *lp)

```
....
75.          perror(NULL);
```

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=1050100&projectid=50090&pathid=2005
Status	New

The system data read by put_sbuf_line in the file src-1/buf.c at line 88 is potentially exposed by put_sbuf_line found in src-1/buf.c at line 88.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	95	95
Object	perror	perror

Code Snippet
File Name src-1/buf.c
Method put_sbuf_line(char *cs)

```
....
95.          perror(NULL);
```

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=1050100&projectid=50090&pathid=2006
Status	New

The system data read by put_sbuf_line in the file src-1/buf.c at line 88 is potentially exposed by put_sbuf_line found in src-1/buf.c at line 88.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	111	111
Object	perror	perror

Code Snippet
File Name src-1/buf.c
Method put_sbuf_line(char *cs)

```
....
111.                    perror(NULL);
```

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=1050100&projectid=50090&pathid=2007
Status New

The system data read by put_sbuf_line in the file src-1/buf.c at line 88 is potentially exposed by put_sbuf_line found in src-1/buf.c at line 88.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	122	122
Object	perror	perror

Code Snippet
File Name src-1/buf.c
Method put_sbuf_line(char *cs)

```
....
122.                perror(NULL);
```

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=1050100&projectid=50090&pathid=2008
Status New

The system data read by open_sbuf in the file src-1/buf.c at line 205 is potentially exposed by open_sbuf found in src-1/buf.c at line 205.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	215	215
Object	perror	perror

Code Snippet
File Name src-1/buf.c
Method open_sbuf(void)

```
....
215.                perror(sfn);
```

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=1050100&projectid=50090&pathid=2009
Status	New

The system data read by close_sbuf in the file src-1/buf.c at line 225 is potentially exposed by close_sbuf found in src-1/buf.c at line 225.

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	229	229
Object	perror	perror

Code Snippet
File Name src-1/buf.c
Method close_sbuf(void)

```
....
229.                    perror(sfn);
```

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=1050100&projectid=50090&pathid=2010
Status	New

The system data read by main in the file src-1/infokey.c at line 91 is potentially exposed by main found in src-1/infokey.c at line 91.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c

Line	101	101
Object	perror	perror

Code Snippet
File Name src-1/infokey.c
Method main (int argc, char **argv)

```
....
101.        perror("pledge");
```

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=1050100&projectid=50090&pathid=2011
Status	New

The system data read by load_server_config in the file src-1/servconf.c at line 2538 is potentially exposed by load_server_config found in src-1/servconf.c at line 2538.

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	2548	2548
Object	perror	perror

Code Snippet
File Name src-1/servconf.c
Method load_server_config(const char *filename, struct sshbuf *conf)

```
....
2548.            perror(filename);
```

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=1050100&projectid=50090&pathid=2012
Status	New

The system data read by do_exec_no_pty in the file src-1/session.c at line 375 is potentially exposed by do_exec_no_pty found in src-1/session.c at line 375.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	459	459
Object	perror	perror

Code Snippet
File Name src-1/session.c
Method do_exec_no_pty(struct ssh *ssh, Session *s, const char *command)

```
....
459.                    perror("dup2 stdin");
```

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=1050100&projectid=50090&pathid=2013
Status	New

The system data read by do_exec_no_pty in the file src-1/session.c at line 375 is potentially exposed by do_exec_no_pty found in src-1/session.c at line 375.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	465	465
Object	perror	perror

Code Snippet
File Name src-1/session.c
Method do_exec_no_pty(struct ssh *ssh, Session *s, const char *command)

```
....
465.                    perror("dup2 stdout");
```

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=1050100&projectid=50090&pathid=2014
Status	New

The system data read by do_exec_no_pty in the file src-1/session.c at line 375 is potentially exposed by do_exec_no_pty found in src-1/session.c at line 375.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	471	471
Object	perror	perror

Code Snippet
File Name src-1/session.c

Method	do_exec_no_pty(struct ssh *ssh, Session *s, const char *command)

```
....
471.                    perror("dup2 stderr");
```

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=1050100&projectid=50090&pathid=2015
Status	New

The system data read by do_setusercontext in the file src-1/session.c at line 1117 is potentially exposed by do_setusercontext found in src-1/session.c at line 1117.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1125	1125
Object	perror	perror

Code Snippet	
File Name	src-1/session.c
Method	do_setusercontext(struct passwd *pw)

```
....
1125.                   perror("unable to set user context");
```

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=1050100&projectid=50090&pathid=2016
Status	New

The system data read by do_setusercontext in the file src-1/session.c at line 1117 is potentially exposed by do_setusercontext found in src-1/session.c at line 1117.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1148	1148
Object	perror	perror

Code Snippet	
File Name	src-1/session.c
Method	do_setusercontext(struct passwd *pw)

```
....
1148.                    perror("unable to set user context (setuser)");
```

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=1050100&projectid=50090&pathid=2017
Status	New

The system data read by do_pwchange in the file src-1/session.c at line 1161 is potentially exposed by do_pwchange found in src-1/session.c at line 1161.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1169	1169
Object	perror	perror

Code Snippet
File Name src-1/session.c
Method do_pwchange(Session *s)

```
....
1169.              perror("passwd");
```

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=1050100&projectid=50090&pathid=2018
Status	New

The system data read by do_child in the file src-1/session.c at line 1226 is potentially exposed by do_child found in src-1/session.c at line 1226.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1374	1374
Object	perror	perror

Code Snippet
File Name src-1/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1374.                   perror(shell);
```

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=1050100&projectid=50090&pathid=2019
Status	New

The system data read by do_child in the file src-1/session.c at line 1226 is potentially exposed by do_child found in src-1/session.c at line 1226.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1384	1384
Object	perror	perror

Code Snippet
File Name src-1/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1384.              perror(shell);
```

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=1050100&projectid=50090&pathid=2020
Status	New

The system data read by do_child in the file src-1/session.c at line 1226 is potentially exposed by do_child found in src-1/session.c at line 1226.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1396	1396
Object	perror	perror

Code Snippet
File Name src-1/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1396.       perror(shell);
```

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=1050100&projectid=50090&pathid=2021
Status	New

The system data read by telnet in the file src-1/telnet.c at line 1839 is potentially exposed by telnet found in src-1/telnet.c at line 1839.

	Source	Destination
File	src-1/telnet.c	src-1/telnet.c
Line	1845	1845
Object	perror	perror

Code Snippet
File Name src-1/telnet.c
Method telnet(char *user)

```
....
1845.       perror("pledge");
```

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=1050100&projectid=50090&pathid=2022
Status	New

The system data read by do_child in the file src-1/session.c at line 1226 is potentially exposed by do_child found in src-1/session.c at line 1226.

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	1317	1315
Object	errno	fprintf

Code Snippet
File Name src-1/session.c
Method do_child(struct ssh *ssh, Session *s, const char *command)

```
....
1317.                       strerror(errno));
....
1315.                   fprintf(stderr, "Could not chdir to home "
```

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=1050100&projectid=50090&pathid=1031
Status	New

The channel_setup_fwd_listener_tcpip method performs a reverse DNS lookup with getnameinfo, at line 3679 of src-1/channels.c. The application then makes a security decision, !=, in src-1/channels.c line 3679, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	3757	3759
Object	getnameinfo	!=

Code Snippet
File Name src-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3757.             if (getnameinfo(ai->ai_addr, ai->ai_addrlen, ntop,
sizeof(ntop),
....
3759.                 NI_NUMERICHOST|NI_NUMERICSERV) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1032
Status	New

The connect_next method performs a reverse DNS lookup with getnameinfo, at line 4473 of src-1/channels.c. The application then makes a security decision, !=, in src-1/channels.c line 4473, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	4490	4492
Object	getnameinfo	!=

Code Snippet
File Name src-1/channels.c
Method connect_next(struct channel_connect *cctx)

```
....
4490.                    if (getnameinfo(cctx->ai->ai_addr, cctx->ai-
>ai_addrlen,
....
4492.                        NI_NUMERICHOST|NI_NUMERICSERV) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1033
Status New

The format_listen_addrs method performs a reverse DNS lookup with getnameinfo, at line 2880 of src-1/servconf.c. The application then makes a security decision, !=, in src-1/servconf.c line 2880, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	2893	2895
Object	getnameinfo	!=

Code Snippet
File Name src-1/servconf.c
Method format_listen_addrs(struct listenaddr *la)

```
....
2893.             if ((r = getnameinfo(ai->ai_addr, ai->ai_addrlen,
addr,
....
2895.                 NI_NUMERICHOST|NI_NUMERICSERV)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 4:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1034
Status	New

The format_listen_addrs method performs a reverse DNS lookup with getnameinfo, at line 2880 of src-1/servconf.c. The application then makes a security decision, r, in src-1/servconf.c line 2880, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	2893	2893
Object	getnameinfo	r

Code Snippet
File Name src-1/servconf.c
Method format_listen_addrs(struct listenaddr *la)

```
....
2893.             if ((r = getnameinfo(ai->ai_addr, ai->ai_addrlen,
addr,
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1035
Status	New

The channel_setup_fwd_listener_tcpip method performs a reverse DNS lookup with getaddrinfo, at line 3679 of src-1/channels.c. The application then makes a security decision, !=, in src-1/channels.c line 3679, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	3722	3722
Object	getaddrinfo	!=

Code Snippet
File Name src-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3722.       if ((r = getaddrinfo(addr, strport, &hints, &aitop)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 6:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1036
Status	New

The channel_setup_fwd_listener_tcpip method performs a reverse DNS lookup with getaddrinfo, at line 3679 of src-1/channels.c. The application then makes a security decision, r, in src-1/channels.c line 3679, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	3722	3722
Object	getaddrinfo	r

Code Snippet
File Name src-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3722.       if ((r = getaddrinfo(addr, strport, &hints, &aitop)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1037
Status	New

The connect_to_helper method performs a reverse DNS lookup with getaddrinfo, at line 4549 of src-1/channels.c. The application then makes a security decision, !=, in src-1/channels.c line 4549, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	4588	4589
Object	getaddrinfo	!=

Code Snippet
File Name src-1/channels.c
Method connect_to_helper(struct ssh *ssh, const char *name, int port, int socktype,

```
....
4588.              if ((gaierr = getaddrinfo(name, strport, &hints,
&cctx->aitop))
4589.                   != 0) {
```

Reliance on DNS Lookups in a Decision\Path 8:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1038
Status	New

The connect_to_helper method performs a reverse DNS lookup with getaddrinfo, at line 4549 of src-1/channels.c. The application then makes a security decision, gaierr, in src-1/channels.c line 4549, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	4588	4588
Object	getaddrinfo	gaierr

Code Snippet
File Name src-1/channels.c
Method connect_to_helper(struct ssh *ssh, const char *name, int port, int socktype,

```
....
4588.             if ((gaierr = getaddrinfo(name, strport, &hints,
&cctx->aitop))
```

Reliance on DNS Lookups in a Decision\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1039
Status	New

The x11_create_display_inet method performs a reverse DNS lookup with getaddrinfo, at line 4890 of src-1/channels.c. The application then makes a security decision, !=, in src-1/channels.c line 4890, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	4913	4914
Object	getaddrinfo	!=

Code Snippet
File Name src-1/channels.c
Method x11_create_display_inet(struct ssh *ssh, int x11_display_offset,

```
....
4913.             if ((gaierr = getaddrinfo(NULL, strport,
4914.                 &hints, &aitop)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1040
Status	New

The x11_create_display_inet method performs a reverse DNS lookup with getaddrinfo, at line 4890 of src-1/channels.c. The application then makes a security decision, gaierr, in src-1/channels.c line 4890, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	4913	4913
Object	getaddrinfo	gaierr

Code Snippet
File Name src-1/channels.c
Method x11_create_display_inet(struct ssh *ssh, int x11_display_offset,

```
....
4913.             if ((gaierr = getaddrinfo(NULL, strport,
```

Reliance on DNS Lookups in a Decision\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1041
Status	New

The x11_connect_display method performs a reverse DNS lookup with getaddrinfo, at line 4999 of src-1/channels.c. The application then makes a security decision, !=, in src-1/channels.c line 4999, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	5066	5066
Object	getaddrinfo	!=

Code Snippet
File Name src-1/channels.c
Method x11_connect_display(struct ssh *ssh)

```
....
5066.       if ((gaierr = getaddrinfo(buf, strport, &hints, &aitop)) !=
0) {
```

Reliance on DNS Lookups in a Decision\Path 12:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1042
Status	New

The x11_connect_display method performs a reverse DNS lookup with getaddrinfo, at line 4999 of src-1/channels.c. The application then makes a security decision, gaierr, in src-1/channels.c line 4999, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/channels.c	src-1/channels.c
Line	5066	5066
Object	getaddrinfo	gaierr

Code Snippet
File Name src-1/channels.c
Method x11_connect_display(struct ssh *ssh)

```
....
5066.       if ((gaierr = getaddrinfo(buf, strport, &hints, &aitop)) !=
0) {
```

Reliance on DNS Lookups in a Decision\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1043
Status	New

The add_one_listen_addr method performs a reverse DNS lookup with getaddrinfo, at line 736 of src-1/servconf.c. The application then makes a security decision, !=, in src-1/servconf.c line 736, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	771	771
Object	getaddrinfo	!=

Code Snippet
File Name src-1/servconf.c
Method add_one_listen_addr(ServerOptions *options, const char *addr,

```
....
771.        if ((gaierr = getaddrinfo(addr, strport, &hints, &aitop)) !=
0)
```

Reliance on DNS Lookups in a Decision\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1044
Status	New

The add_one_listen_addr method performs a reverse DNS lookup with getaddrinfo, at line 736 of src-1/servconf.c. The application then makes a security decision, gaierr, in src-1/servconf.c line 736, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	src-1/servconf.c	src-1/servconf.c
Line	771	771
Object	getaddrinfo	gaierr

Code Snippet
File Name src-1/servconf.c
Method add_one_listen_addr(ServerOptions *options, const char *addr,

```
....
771.        if ((gaierr = getaddrinfo(addr, strport, &hints, &aitop)) !=
0)
```

Use of Obsolete Functions

Query Path:
CPP\Cx\CPP Low Visibility\Use of Obsolete Functions Version:0

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities

Description

Use of Obsolete Functions\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1209
Status	New

Method mrsetlow in src-1/i686_mem.c, at line 394, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/i686_mem.c	src-1/i686_mem.c
Line	413	413
Object	bcopy	bcopy

Code Snippet
File Name src-1/i686_mem.c

Method	mrsetlow(struct mem_range_softc *sc, struct mem_range_desc *mrd, int *arg)

```
....
413.              bcopy(mrd->mr_owner, curr_md->mr_owner, sizeof(mrd-
>mr_owner));
```

Use of Obsolete Functions\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1210
Status	New

Method mrsetvariable in src-1/i686_mem.c, at line 424, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/i686_mem.c	src-1/i686_mem.c
Line	472	472
Object	bcopy	bcopy

Code Snippet	
File Name	src-1/i686_mem.c
Method	mrsetvariable(struct mem_range_softc *sc, struct mem_range_desc *mrd, int *arg)

```
....
472.        bcopy(mrd->mr_owner, free_md->mr_owner, sizeof(mrd-
>mr_owner));
```

Use of Obsolete Functions\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1211
Status	New

Method parent_dispatch_hce in src-1/relayd.c, at line 442, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	451	451
Object	bcopy	bcopy

Code Snippet	
File Name	src-1/relayd.c
Method	parent_dispatch_hce(int fd, struct privsep_proc *p, struct imsg *imsg)

```
....
451.              bcopy(imsg->data, &scr, sizeof(scr));
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1212
Status	New

Method parent_dispatch_relay in src-1/relayd.c, at line 466, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	476	476
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method parent_dispatch_relay(int fd, struct privsep_proc *p, struct imsg *imsg)

```
....
476.              bcopy(imsg->data, &bnd, sizeof(bnd));
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1213
Status	New

Method table_findbyconf in src-1/relayd.c, at line 1163, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1168	1168
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method table_findbyconf(struct relayd *env, struct table *tb)

```
....
1168.       bcopy(&tb->conf, &a, sizeof(a));
```

Use of Obsolete Functions\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1214
Status	New

Method table_findbyconf in src-1/relayd.c, at line 1163, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1173	1173
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method table_findbyconf(struct relayd *env, struct table *tb)

```
....
1173.             bcopy(&table->conf, &b, sizeof(b));
```

Use of Obsolete Functions\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1215
Status	New

Method event_again in src-1/relayd.c, at line 1432, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1439	1439
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method event_again(struct event *ev, int fd, short event,

```
....
1439.       bcopy(end, &tv_next, sizeof(tv_next));
```

Use of Obsolete Functions\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=500

	90&pathid=1216
Status	New

Method event_again in src-1/relayd.c, at line 1432, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1445	1445
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method event_again(struct event *ev, int fd, short event,

```
....
1445.             bcopy(&tv_next, &tv, sizeof(tv));
```

Use of Obsolete Functions\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1217
Status	New

Method map6to4 in src-1/relayd.c, at line 1658, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1669	1669
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method map6to4(struct sockaddr_storage *in6)

```
....
1669.       bcopy(&sin6->sin6_addr.s6_addr[12], &sin4->sin_addr.s_addr,
```

Use of Obsolete Functions\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1218
Status	New

Method map6to4 in src-1/relayd.c, at line 1658, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1677	1677
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method map6to4(struct sockaddr_storage *in6)

```
....
1677.       bcopy(&out4, in6, sizeof(*in6));
```

Use of Obsolete Functions\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1219
Status	New

Method map4to6 in src-1/relayd.c, at line 1683, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1695	1695
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method map4to6(struct sockaddr_storage *in4, struct sockaddr_storage *map)

```
....
1695.       bcopy(map6, sin6, sizeof(*sin6));
```

Use of Obsolete Functions\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1220
Status	New

Method map4to6 in src-1/relayd.c, at line 1683, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1700	1700

Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method map4to6(struct sockaddr_storage *in4, struct sockaddr_storage *map)

```
....
1700.       bcopy(&sin4->sin_addr.s_addr, &sin6->sin6_addr.s6_addr[12],
```

Use of Obsolete Functions\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1221
Status	New

Method map4to6 in src-1/relayd.c, at line 1683, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	1703	1703
Object	bcopy	bcopy

Code Snippet
File Name src-1/relayd.c
Method map4to6(struct sockaddr_storage *in4, struct sockaddr_storage *map)

```
....
1703.       bcopy(&out6, in4, sizeof(*in4));
```

Use of Obsolete Functions\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1222
Status	New

Method rl_attach in src-1/rtl81x9.c, at line 1101, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	src-1/rtl81x9.c	src-1/rtl81x9.c
Line	1189	1189
Object	bcopy	bcopy

Code Snippet
File Name src-1/rtl81x9.c

Method	rl_attach(struct rl_softc *sc)

```
....
1189.       bcopy(sc->sc_dev.dv_xname, ifp->if_xname, IFNAMSIZ);
```

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=1050100&projectid=50090&pathid=1021
Status	New

The buffer allocated by <= in src-1/csqrt_test.c at line 252 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/csqrt_test.c	src-1/csqrt_test.c
Line	270	270
Object	<=	<=

Code Snippet	
File Name	src-1/csqrt_test.c
Method	test_precision(int maxexp, int mantdig)

```
....
270.        for (exp = 0; exp <= maxexp; exp += 2) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1022
Status	New

The buffer allocated by <= in src-1/glob.c at line 246 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	src-1/glob.c	src-1/glob.c
Line	285	285
Object	<=	<=

Code Snippet
File Name src-1/glob.c
Method globexp2(const Char *ptr, const Char *pattern, glob_t *pglob,

```
....
285.        for (i = 0, pl = pm = ptr; pm <= pe; pm++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1023
Status	New

The buffer allocated by <= in src-1/kern_proc.c at line 652 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/kern_proc.c	src-1/kern_proc.c
Line	658	658
Object	<=	<=

Code Snippet
File Name src-1/kern_proc.c
Method pgrpdump(void)

```
....
658.        for (i = 0; i <= pgrphash; 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=1050100&projectid=50090&pathid=1024
Status	New

The buffer allocated by <= in src-1/nl.c at line 235 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/nl.c	src-1/nl.c
Line	252	252

Object	<=	<=

Code Snippet
File Name src-1/nl.c
Method filter(void)

```
....
252.              for (idx = FOOTER; idx <= NP_LAST; idx++) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1025
Status	New

The buffer allocated by <= in src-1/pfkdump.c at line 694 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/pfkdump.c	src-1/pfkdump.c
Line	874	874
Object	<=	<=

Code Snippet
File Name src-1/pfkdump.c
Method pfkey_print_sa(struct sadb_msg *msg, int opts)

```
....
874.              for (i = 0; i <= SADB_EXT_MAX; i++)
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1026
Status	New

The buffer allocated by <= in src-1/pfkdump.c at line 882 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/pfkdump.c	src-1/pfkdump.c
Line	897	897
Object	<=	<=

Code Snippet	
File Name	src-1/pfkdump.c
Method	pfkey_monitor_sa(struct sadb_msg *msg, int opts)

```
....
897.        for (i = 0; i <= SADB_EXT_MAX; i++)
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1027
Status	New

The buffer allocated by <= in src-1/remote-st.c at line 413 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/remote-st.c	src-1/remote-st.c
Line	420	420
Object	<=	<=

Code Snippet	
File Name	src-1/remote-st.c
Method	st2000_fetch_registers (void)

```
....
420.    for (regno = 0; regno <= PC_REGNUM; regno++)
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1028
Status	New

The buffer allocated by <= in src-1/remote-st.c at line 446 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/remote-st.c	src-1/remote-st.c
Line	450	450
Object	<=	<=

Code Snippet	
File Name	src-1/remote-st.c
Method	st2000_store_registers (void)

```
....
450.    for (regno = 0; regno <= PC_REGNUM; regno++)
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1029
Status	New

The buffer allocated by <= in src-1/remote-st.c at line 603 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/remote-st.c	src-1/remote-st.c
Line	611	611
Object	<=	<=

Code Snippet
File Name src-1/remote-st.c
Method st2000_insert_breakpoint (CORE_ADDR addr, char *shadow)

```
....
611.    for (i = 0; i <= MAX_STDEBUG_BREAKPOINTS; i++)
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1030
Status	New

The buffer allocated by <= in src-1/rt2860.c at line 769 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	src-1/rt2860.c	src-1/rt2860.c
Line	783	783
Object	<=	<=

Code Snippet
File Name src-1/rt2860.c
Method rt2860_media_change(struct ifnet *ifp)

```
....
783.              for (ridx = 0; ridx <= RT2860_RIDX_MAX; ridx++)
```

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=1050100&projectid=50090&pathid=834
Status	New

	Source	Destination
File	src-1/ls.c	src-1/ls.c
Line	135	135
Object	getopt	getopt

Code Snippet
File Name src-1/ls.c
Method ls_main(int argc, char *argv[])

```
....
135.        while ((ch = getopt(argc, argv,
"1ACFHLRSTacdfghiklmnopqrstux")) != -1) {
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=835
Status	New

	Source	Destination
File	src-1/nl.c	src-1/nl.c
Line	124	124
Object	getopt	getopt

Code Snippet
File Name src-1/nl.c
Method main(int argc, char *argv[])

```
....
124.        while ((c = getopt(argc, argv, "pb:d:f:h:i:l:n:s:v:w:")) !=
-1) {
```

Inconsistent Implementations\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=836
Status	New

	Source	Destination
File	src-1/relayd.c	src-1/relayd.c
Line	132	132
Object	getopt	getopt

Code Snippet
File Name src-1/relayd.c
Method main(int argc, char *argv[])

```
....
132.        while ((c = getopt(argc, argv, "dD:nI:P:f:v")) != -1) {
```

Inconsistent Implementations\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=837
Status	New

	Source	Destination
File	src-1/tmux.c	src-1/tmux.c
Line	374	374
Object	getopt	getopt

Code Snippet
File Name src-1/tmux.c
Method main(int argc, char **argv)

```
....
374.        while ((opt = getopt(argc, argv, "2c:CDdf:lL:NqS:T:uUvV"))
!= -1) {
```

Inconsistent Implementations\Path 5:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=838
Status	New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	271	271
Object	getopt	getopt

Code Snippet
File Name src-1/unifdef.c
Method main(int argc, char *argv[])

```
....
271.        while ((opt = getopt(argc, argv,
"i:D:U:f:I:M:o:x:bBcdehKklmnsStV")) != -1)
```

Inconsistent Implementations\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=839
Status	New

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	116	116
Object	getopt_long	getopt_long

Code Snippet
File Name src-1/infokey.c
Method main (int argc, char **argv)

```
....
116.        (argc, argv, short_options, long_options,
&getopt_long_index);
```

Insecure Temporary File

Query Path:
CPP\Cx\CPP Low Visibility\Insecure Temporary File Version:0

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insecure Temporary File\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1223
Status	New

	Source	Destination
File	src-1/buf.c	src-1/buf.c
Line	211	211
Object	mkstemp	mkstemp

Code Snippet
File Name src-1/buf.c
Method open_sbuf(void)

```
....
211.        if ((fd = mkstemp(sfn)) == -1 ||
```

Insecure Temporary File\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1224
Status	New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	743	743
Object	mkstemp	mkstemp

Code Snippet
File Name src-1/server.c
Method recvfile(char *new, opt_t opts, int mode, char *owner, char *group,

```
....
743.        if (chkparent(new, opts) < 0 || (f = mkstemp(new)) == -1) {
```

Insecure Temporary File\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1225
Status	New

	Source	Destination
File	src-1/session.c	src-1/session.c
Line	256	256
Object	mkstemp	mkstemp

Code Snippet
File Name src-1/session.c
Method prepare_auth_info_file(struct passwd *pw, struct sshbuf *info)

```
....
256.        if ((fd = mkstemp(auth_info_file)) == -1) {
```

Insecure Temporary File\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1226
Status New

	Source	Destination
File	src-1/unifdef.c	src-1/unifdef.c
Line	1587	1587
Object	mkstemp	mkstemp

Code Snippet
File Name src-1/unifdef.c
Method mktempmode(char *tmp, int mode)

```
....
1587.       int fd = mkstemp(tmp);
```

Insecure Temporary File\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1227
Status New

	Source	Destination
File	src-1/server.c	src-1/server.c
Line	1151	1151
Object	mktemp	mktemp

Code Snippet

File Name	src-1/server.c
Method	recvlink(char *new, opt_t opts, int mode, off_t size)

```
....
1151.       if (chkparent(new, opts) < 0 || mktemp(new) == NULL ||
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow read\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1204
Status	New

The size of the buffer used by ax_recv in BinaryExpr, at line 98 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_recv passes to BinaryExpr, at line 98 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	115	156
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	src-1/ax.c
Method	ax_recv(struct ax *ax)

```
....
115.              if ((nread = read(ax->ax_fd, ax->ax_rbuf + ax-
>ax_rblen,
....
156.                   header.aph_plength - (ax->ax_rblen -
AX_PDU_HEADER));
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1205
Status	New

The size of the buffer used by ax_recv in BinaryExpr, at line 98 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_recv passes to BinaryExpr, at line 98 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	115	156
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
115.              if ((nread = read(ax->ax_fd, ax->ax_rbuf + ax-
>ax_rblen,
....
156.                  header.aph_plength - (ax->ax_rblen -
AX_PDU_HEADER));
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1206
Status New

The size of the buffer used by ax_recv in ax_rblen, at line 98 of src-1/ax.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ax_recv passes to BinaryExpr, at line 98 of src-1/ax.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ax.c	src-1/ax.c
Line	115	156
Object	BinaryExpr	ax_rblen

Code Snippet
File Name src-1/ax.c
Method ax_recv(struct ax *ax)

```
....
115.              if ((nread = read(ax->ax_fd, ax->ax_rbuf + ax-
>ax_rblen,
....
156.                  header.aph_plength - (ax->ax_rblen -
AX_PDU_HEADER));
```

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=1050100&projectid=50090&pathid=840
Status	New

Method main at line 91 of src-1/infokey.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 91 of src-1/infokey.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	src-1/infokey.c	src-1/infokey.c
Line	91	203
Object	argv	input_filename

Code Snippet
File Name src-1/infokey.c
Method main (int argc, char **argv)

```
....
91.  main (int argc, char **argv)
....
203.       inf = fopen (input_filename, "r");
```

Potential Path Traversal\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=841
Status	New

Method main at line 116 of src-1/maketab.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 116 of src-1/maketab.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	src-1/maketab.c	src-1/maketab.c
Line	116	133
Object	argv	argv

Code Snippet
File Name src-1/maketab.c
Method int main(int argc, char *argv[])

```
....
116.  int main(int argc, char *argv[])
....
133.        if ((fp = fopen(argv[1], "r")) == NULL) {
```

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=1050100&projectid=50090&pathid=1207
Status	New

The size of the buffer used by ipseckey_has_safe_characters in "%d %d %d %s ", at line 215 of src-1/ipsecmod.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ipseckey_has_safe_characters passes to "%d %d %d %s ", at line 215 of src-1/ipsecmod.c, to overwrite the target buffer.

	Source	Destination
File	src-1/ipsecmod.c	src-1/ipsecmod.c
Line	223	223
Object	"%d %d %d %s "	"%d %d %d %s "

Code Snippet
File Name src-1/ipsecmod.c
Method ipseckey_has_safe_characters(char* s, size_t slen) {

```
....
223.        if(sscanf(s, "%d %d %d %s ",
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=1208
Status	New

The size of the buffer used by st2000_open in " %s %d %s", at line 272 of src-1/remote-st.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that st2000_open passes to " %s %d %s", at line 272 of src-1/remote-st.c, to overwrite the target buffer.

	Source	Destination

File	src-1/remote-st.c	src-1/remote-st.c
Line	279	279
Object	" %s %d %s"	" %s %d %s"

Code Snippet
File Name src-1/remote-st.c
Method st2000_open (char *args, int from_tty)

```
....
279.    n = sscanf (args, " %s %d %s", dev_name, &baudrate, junk);
```

Information Exposure Through Comments

Query Path:
CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description
Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050100&projectid=50090&pathid=2051
Status	New

	Source	Destination
File	src-1/ssl_srvr.c	src-1/ssl_srvr.c
Line	1161	1161
Object	cipher -	cipher -

Code Snippet
File Name src-1/ssl_srvr.c
Method * s->hs.cipher - the new cipher to use.

```
....
1161.        * s->hs.cipher   - the new cipher to use.
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow Indexes

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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

Off by One Error in Arrays

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Resource Injection

Risk

What might happen

An attacker might be able to open a backdoor enabling the attacker to connect directly to the application server, potentially leading to server takeover or other indirect attacks. In particular, by modifying the socket port number, an attacker may be able to bypass incomplete network controls or obfuscate the attack from network devices.

Furthermore, this flaw can be exploited to bypass firewalls or other access control mechanisms; to use the application as a proxy for port scanning of internal networks and direct access to local systems; or to misdirect the user into sending sensitive information to a bogus server.

Cause

How does it happen

The application opens a network socket, for listening for incoming network connections. However, the application uses untrusted data to configure the socket, enabling an attacker to control it.

General Recommendations

How to avoid it

- Do not allow a user or untrusted data to define parameters of network sockets or other network settings.
- Likewise, do not allow user-controlled input or untrusted data to define environment variables or file locations.

Source Code Examples

CPP

Open Socket and Connect to Remote Server on User-Defined Port

```
int main( int argc, char* argv[] )
{
	int sockfd, portno;
	struct sockaddr_in serv_addr = {};
	struct hostent *server;

	if ( argc != 3 )
		errorAndExit();

	server = gethostbyname(argv[1]);
	if (server == NULL)
		errorAndExit();

	portno = atoi(argv[2]);

	serv_addr.sin_family = AF_INET;
	memcpy(&serv_addr.sin_addr.s_addr, server->h_addr, server->h_length);
	serv_addr.sin_port = htons(portno);
```

```
	sockfd = socket(AF_INET, SOCK_STREAM, 0);
	if (sockfd < 0)
		errorAndExit();

	if (connect(sockfd, &serv_addr, sizeof(serv_addr)) < 0)
		errorAndExit();

	sendAndProcessMessage(sockfd);

	close(sockfd);
}
```

Select Port for Socket Binding From Hardcoded List

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

{
	int sockfd, portno;
	struct sockaddr_in serv_addr = {};
	char* portname;

	if ( argc != 1 )
		errorAndExit();

	portname = argv[1];
	switch (portname) {
		case "quicktime":
			portno = 1220;
			break;
		case "kazaa":
			portno = 1214;
			break;
		case "battlenet":
			portno = 1119;
			break;
		default:
			portno = 80;
	}

	serv_addr.sin_family = AF_INET;
	memcpy(&serv_addr.sin_addr.s_addr, SERVER_ADDRESS, strlen(SERVER_ADDRESS));
	serv_addr.sin_port = htons(portno);

	sockfd = socket(AF_INET, SOCK_STREAM, 0);
	if (sockfd < 0)
		errorAndExit();

	if (connect(sockfd, &serv_addr, sizeof(serv_addr)) < 0)
		errorAndExit();

	sendAndProcessMessage(sockfd);

	close(sockfd);
}
```

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

Buffer Overflow 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

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

Boolean 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

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

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

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;

  void setPassword()
```

```
  {
      password = System.console().readLine("Enter your password: ");
   }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed

{
  private SealedObject password;

  void setPassword()

 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
```

```
	gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
	char* password = (char*) malloc(256);
	int i=0;
	char ch;
	ssize_t k;
	while(k = read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n'){
			password[i]='\0';
			break;
		} else{
			password[i++]=ch;
			fflush(0);
		}
	}
	i=0;
	memset(password,'\0',256);
}

int main()

{

	printf("Please enter a password:\n");
	authfunc();
	somefunc();
	char ch;
	while(read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n')
			break;
	}
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obselete since it is relatively easy to break. These obselete algorithms are vulnerable to several different kinds of attacks, including brute force.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.
- Do not use weak, outdated, or obsolete algorithms.
- Ensure you select the correct cryptographic mechanism according to the specific requirements.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
- Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
- Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
- For symmetric encryption, use a key length of at least 256 bits.

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.md5Hex(socialSecurityNum);
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.sha256Hex(socialSecurityNum);
}
```

Use of 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 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

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
```

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

Heuristic 2nd Order Buffer Overflow read

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Use of Obsolete Functions

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

Java

Using Deprecated Methods for Security Checks

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        secManager.checkMulticast(address, 0)
    }

}
```

A Replacement Security Check

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        SocketPermission permission = new SocketPermission(address.getHostAddress(),
"accept,connect");

        secManager.checkPermission(permission)
    }
```

```
}
```

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in

the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

BACK TO TOP

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

Information Leak Through Comments

Weakness ID: 615 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

- Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

Reference	Description
CVE-2007-6197	Version numbers and internal hostnames leaked in HTML comments.
CVE-2007-4072	CMS places full pathname of server in HTML comment.
CVE-2009-2431	blog software leaks real username in HTML comment.

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	**Development Concepts (primary)699 Research Concepts (primary)1000**

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	Anonymous Tool Vendor (under NDA)		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal

	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	6/19/2024
Common	0105849645654507	6/19/2024