ravynos-1 Scan Report

Project Name	ravynos-1
Scan Start	Saturday, June 22, 2024 9:07:38 AM
Preset	Checkmarx Default
Scan Time	00h:24m:04s
Lines Of Code Scanned	299790
Files Scanned	113
Report Creation Time	Saturday, June 22, 2024 9:43:16 AM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	6/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

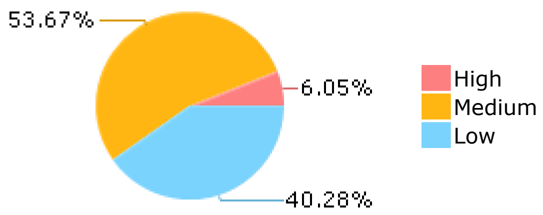
Results Limit

Results limit per query was set to 50

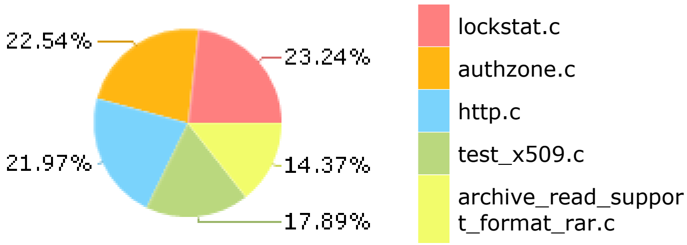
Selected Queries

Selected queries are listed in Result Summary

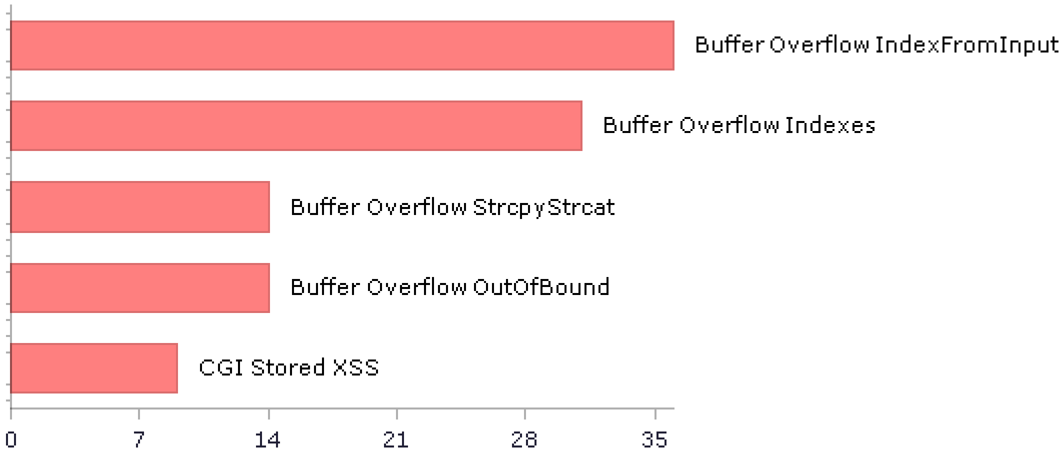
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	545	311
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	160	160
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	28	17
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	11	3
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	9	3
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	392	392
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	9	3
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	11	3
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	3	3
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	392	392
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	10	10
PCI DSS (3.2) - 6.5.2 - Buffer overflows	315	255
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)	9	3
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.	12	12
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.	31	20
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	166	160
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.	9	9
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.	33	27

* 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)	176	176
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)	15	4
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*****	16	10
SC-28 Protection of Information at Rest (P1)	8	8
SC-4 Information in Shared Resources (P1)	5	5
SC-5 Denial of Service Protection (P1)*****	346	157
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	230	162
SI-11 Error Handling (P2)*****	121	121
SI-15 Information Output Filtering (P0)	9	3
SI-16 Memory Protection (P1)	64	14

***** 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

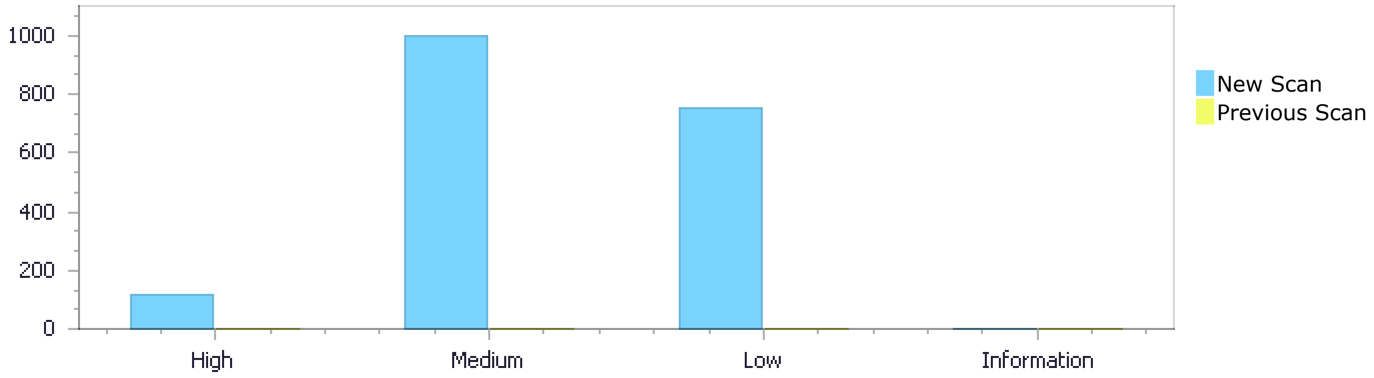
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	113	1,002	752	0	1,867
Recurrent Issues	0	0	0	0	0
Total	113	1,002	752	0	1,867

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	113	1,002	752	0	1,867
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	113	1,002	752	0	1,867

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	36	High
Buffer Overflow Indexes	31	High
Buffer Overflow OutOfBound	14	High
Buffer Overflow StrcpyStrcat	14	High
CGI Stored XSS	9	High

Buffer Overflow boundedcpy	4	High
Buffer Overflow LongString	4	High
Command Injection	1	High
Dangerous Functions	363	Medium
Buffer Overflow boundcpy WrongSizeParam	196	Medium
Memory Leak	83	Medium
Use of Zero Initialized Pointer	81	Medium
MemoryFree on StackVariable	68	Medium
Wrong Size t Allocation	62	Medium
Double Free	55	Medium
Integer Overflow	19	Medium
Inadequate Encryption Strength	15	Medium
Char Overflow	13	Medium
Divide By Zero	12	Medium
Path Traversal	11	Medium
Stored Buffer Overflow boundcpy	9	Medium
Long Overflow	4	Medium
Stored Buffer Overflow cpycat	3	Medium
Wrong Memory Allocation	3	Medium
Buffer Overflow AddressOfLocalVarReturned	2	Medium
Heap Inspection	2	Medium
Use of Uninitialized Pointer	1	Medium
NULL Pointer Dereference	179	Low
Improper Resource Access Authorization	148	Low
Unchecked Return Value	121	Low
Unchecked Array Index	68	Low
Use of Sizeof On a Pointer Type	35	Low
Potential Precision Problem	29	Low
Sizeof Pointer Argument	29	Low
Use of Obsolete Functions	29	Low
TOCTOU	22	Low
Exposure of System Data to Unauthorized Control Sphere	16	Low
Reliance on DNS Lookups in a Decision	16	Low
Inconsistent Implementations	13	Low
Heuristic Buffer Overflow malloc	12	Low
Incorrect Permission Assignment For Critical Resources	12	Low
Potential Off by One Error in Loops	9	Low
Use of Insufficiently Random Values	7	Low
Heuristic 2nd Order Buffer Overflow malloc	2	Low
Insecure Temporary File	2	Low
Information Exposure Through Comments	1	Low
Leaving Temporary Files	1	Low
Privacy Violation	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
ravynos-1/http.c	133
ravynos-1/authzone.c	114

ravynos-1/archive_read_support_format_rar.c	101
ravynos-1/pmcstudy.c	65
ravynos-1/lockstat.c	63
ravynos-1/test_x509.c	56
ravynos-1/mrsas.c	54
ravynos-1/dp_rx.c	43
ravynos-1/name.c	38
ravynos-1/sctp_sys_calls.c	32

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=54
Status	New

The size of the buffer used by show_struct in first_word, at line 1471 of ravynos-1/cxgbetool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 3666 of ravynos-1/cxgbetool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	1486
Object	argv	first_word

Code Snippet
File Name ravynos-1/cxgbetool.c
Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name ravynos-1/cxgbetool.c
Method show_struct(const uint32_t *words, int nwords, const struct field_desc *fd)

```
....
1486.              data = (words[first_word] >> shift) |
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=55
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	991
Object	getenv	BinaryExpr

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                        } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
991.                  dst[3] = base64[(t >> 0) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=56
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	991
Object	getenv	BinaryExpr

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                        } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
991.                dst[3] = base64[(t >> 0) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=57
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	991
Object	getenv	BinaryExpr

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                    } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
991.                dst[3] = base64[(t >> 0) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=58
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	990
Object	getenv	BinaryExpr

Code Snippet
File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                  } else if ((p = getenv("HTTP_PROXY_AUTH")) != 
NULL &&
```

▼

File Name	ravynos-1/http.c

Method	http_base64(const char *src)

```
....
990.             dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=59
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	990
Object	getenv	BinaryExpr

Code Snippet
File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                  } else if ((p = getenv("HTTP_PROXY_AUTH")) != 
NULL &&
```

▼

File Name	ravynos-1/http.c

Method	http_base64(const char *src)

```
....
990.                dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=60
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	990
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
990.                dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=61
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	989

Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
989.                dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=62
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	989
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
989.                dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=63
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	989
Object	getenv	BinaryExpr

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
989.                dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=64
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	988
Object	getenv	BinaryExpr

Code Snippet

File Name ravynos-1/http.c

Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
988.                dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=65
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	988
Object	getenv	BinaryExpr

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
988.                dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=66
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	988
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
988.              dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=67
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1001
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                 } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1001.             dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=68
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	1001
Object	getenv	BinaryExpr

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                 } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1001.             dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=69

Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1001
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                        } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1001.                  dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=70
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1000
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                        } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1000.              dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=71
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	1000
Object	getenv	BinaryExpr

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1000.              dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=72
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1000
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1000.            dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=73
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	999
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
999.             dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=74
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	999
Object	getenv	BinaryExpr

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
999.             dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=75
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c

Line	1724	999
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                    } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
999.               dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=76
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1008
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) != 
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1008.              dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=77
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	1008
Object	getenv	BinaryExpr

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1008.              dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=78
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1008
Object	getenv	BinaryExpr

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1008.              dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=79
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1007
Object	getenv	BinaryExpr

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1007.              dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=80
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	1007
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1007.               dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=81
Status	New

The size of the buffer used by http_base64 in BinaryExpr, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1007
Object	getenv	BinaryExpr

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1007.             dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow IndexFromInput\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=82
Status	New

The size of the buffer used by SB_append_char in PostfixExpr, at line 126 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	651	129
Object	fgetc	PostfixExpr

Code Snippet

File Name ravynos-1/test_x509.c

Method conf_next_low(void)

```
....
651.              x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_append_char(string_builder *sb, int c)

```
....
129.        sb->buf[sb->ptr ++] = c;
```

Buffer Overflow IndexFromInput\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=83
Status	New

The size of the buffer used by SB_append_char in PostfixExpr, at line 126 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	657	129
Object	fgetc	PostfixExpr

Code Snippet

File Name ravynos-1/test_x509.c

Method conf_next_low(void)

```
....
657.                  x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_append_char(string_builder *sb, int c)

```
....
129.            sb->buf[sb->ptr ++] = c;
```

Buffer Overflow IndexFromInput\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=84
Status	New

The size of the buffer used by read_a_line in i, at line 2155 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_a_line passes to buffer, at line 2155 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2160	2166
Object	buffer	i

Code Snippet

File Name ravynos-1/pmcstudy.c

Method read_a_line(FILE *io)

```
....
2160.       if (fgets(buffer, sizeof(buffer), io) == NULL) {
....
2166.             cnts[i].vals[pos] = strtol(p, &stop, 0);
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=85
Status	New

The size of the buffer used by read_a_line in i, at line 2155 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_a_line passes to buffer, at line 2155 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2160	2168
Object	buffer	i

Code Snippet
File Name ravynos-1/pmcstudy.c
Method read_a_line(FILE *io)

```
....
2160.        if (fgets(buffer, sizeof(buffer), io) == NULL) {
....
2168.              cnts[i].sum += cnts[i].vals[pos];
```

Buffer Overflow IndexFromInput\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=86
Status	New

The size of the buffer used by run_test_case in u, at line 1457 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_all passes to BinaryExpr, at line 403 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	423	1521
Object	BinaryExpr	u

Code Snippet
File Name ravynos-1/test_x509.c
Method read_all(FILE *f, size_t *len)

```
....
423.                rlen = fread(buf + ptr, 1, blen - ptr, f);
```

File Name ravynos-1/test_x509.c

Method	run_test_case(test_case *tc)

```
....
1521.                 certs[u].data = read_file(tc->cert_names[u],
&certs[u].len);
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=87
Status	New

The size of the buffer used by run_test_case in u, at line 1457 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_all passes to BinaryExpr, at line 403 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	423	1601
Object	BinaryExpr	u

Code Snippet

File Name	ravynos-1/test_x509.c
Method	read_all(FILE *f, size_t *len)

```
....
423.                  rlen = fread(buf + ptr, 1, blen - ptr, f);
```

File Name	ravynos-1/test_x509.c
Method	run_test_case(test_case *tc)

```
....
1601.                                     certs[u].data + v, w);
```

Buffer Overflow IndexFromInput\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=88
Status	New

The size of the buffer used by run_test_case in u, at line 1457 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_all passes to BinaryExpr, at line 403 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	423	1670
Object	BinaryExpr	u

Code Snippet
File Name ravynos-1/test_x509.c
Method read_all(FILE *f, size_t *len)

```
....
423.                  rlen = fread(buf + ptr, 1, blen - ptr, f);
```

File Name ravynos-1/test_x509.c

Method run_test_case(test_case *tc)

```
....
1670.                 xfree(certs[u].data);
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=89
Status	New

The size of the buffer used by run_cmd_loop in n, at line 1695 of ravynos-1/cxgbtool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_cmd_loop passes to buf, at line 1695 of ravynos-1/cxgbtool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1715	1722
Object	buf	n

Code Snippet
File Name ravynos-1/cxgbtool.c
Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1715.                 n = read(STDIN_FILENO, buf, sizeof(buf) - 1);
....
1722.                       buf[n] = 0;
```

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=1070095&projectid=70085&pathid=5
Status	New

The size of the buffer used by show_struct in first_word, at line 1471 of ravynos-1/cxgbetool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 3666 of ravynos-1/cxgbetool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	1489
Object	argv	first_word

Code Snippet
File Name ravynos-1/cxgbetool.c
Method main(int argc, const char *argv[])

```
....
3666.   main(int argc, const char *argv[])
```

File Name ravynos-1/cxgbetool.c

Method show_struct(const uint32_t *words, int nwords, const struct field_desc *fd)

```
....
1489.                  data |= ((uint64_t)words[first_word + 2] << (64
- shift));
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=6
Status	New

The size of the buffer used by show_struct in first_word, at line 1471 of ravynos-1/cxgbetool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 3666 of ravynos-1/cxgbetool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c

Line	3666	1487
Object	argv	first_word

Code Snippet
File Name   ravynos-1/cxgbetool.c
Method   main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name   ravynos-1/cxgbetool.c

Method   show_struct(const uint32_t *words, int nwords, const struct field_desc *fd)

```
....
1487.                   ((uint64_t)words[first_word + 1] << (32 -
shift));
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=7
Status	New

The size of the buffer used by show_struct in first_word, at line 1471 of ravynos-1/cxgbetool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 3666 of ravynos-1/cxgbetool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	1486
Object	argv	first_word

Code Snippet
File Name   ravynos-1/cxgbetool.c
Method   main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name   ravynos-1/cxgbetool.c

Method   show_struct(const uint32_t *words, int nwords, const struct field_desc *fd)

```
....
1486.               data = (words[first_word] >> shift) |
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=8
Status	New

The size of the buffer used by parse_offload_policy_line in llen, at line 3268 of ravynos-1/cxgbetool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 3666 of ravynos-1/cxgbetool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	3279
Object	argv	llen

Code Snippet

File Name ravynos-1/cxgbetool.c

Method main(int argc, const char *argv[])

```
....
3666.   main(int argc, const char *argv[])
```

File Name ravynos-1/cxgbetool.c

Method parse_offload_policy_line(size_t lno, char *line, size_t llen, pcap_t *pd,

```
....
3279.         s = &line[llen - 1];
```

Buffer Overflow Indexes\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=9
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	991
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
991.               dst[3] = base64[(t >> 0) & 0x3f];
```

Buffer Overflow Indexes\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=10
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	990
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
990.               dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow Indexes\Path 7:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=11
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	989
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
989.                dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=12
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	988
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
988.              dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=13
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1001
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1001.             dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=14

Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1000
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1000.               dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=15
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	999
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
999.                    dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=16
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1008
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1008.                   dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=17
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_connect passes to getenv, at line 1379 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1423	1007
Object	getenv	t

Code Snippet

File Name ravynos-1/http.c

Method http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1423.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1007.             dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=18
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	991
Object	getenv	t

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                   } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
991.                dst[3] = base64[(t >> 0) & 0x3f];
```

Buffer Overflow Indexes\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=19
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	990
Object	getenv	t

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
990.                dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow Indexes\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=20
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c

Line	1694	989
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
989.               dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=21
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	988
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
988.                dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=22
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	1001
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                       } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c
Method http_base64(const char *src)

```
....
1001.               dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow Indexes\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=23
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c

Line	1694	1000
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1000.              dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=24
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	999
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                    } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
999.                dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=25
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1694	1008
Object	getenv	t

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                           } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1008.               dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=26
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c

Line	1694	1007
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1694.                     } else if ((p = getenv("HTTP_PROXY_AUTH")) !=
NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1007.                dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=27
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	991
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                     } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
991.                 dst[3] = base64[(t >> 0) & 0x3f];
```

Buffer Overflow Indexes\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=28
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	990
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
990.                dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow Indexes\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=29
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	989
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                      } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
989.                dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=30
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	988
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                      } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
988.                dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=31

Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1001
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1001.              dst[2] = base64[(t >> 6) & 0x3f];
```

Buffer Overflow Indexes\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=32
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1000
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
1000.               dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=33
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	999
Object	getenv	t

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                     } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

File Name	ravynos-1/http.c
Method	http_base64(const char *src)

```
....
999.                dst[0] = base64[(t >> 18) & 0x3f];
```

Buffer Overflow Indexes\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=34
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1008
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1008.               dst[1] = base64[(t >> 12) & 0x3f];
```

Buffer Overflow Indexes\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=35
Status	New

The size of the buffer used by http_base64 in t, at line 971 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1724	1007
Object	getenv	t

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1724.                   } else if ((p = getenv("HTTP_AUTH")) != NULL &&
```

▼

File Name ravynos-1/http.c

Method http_base64(const char *src)

```
....
1007.               dst[0] = base64[(t >> 18) & 0x3f];
```

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=1070095&projectid=70085&pathid=40
Status	New

The size of the buffer used by http_request_body in pwd, at line 1585 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	1919
Object	getenv	pwd

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

▼

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1919.                             strcpy(new->pwd, url->pwd);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=41
Status	New

The size of the buffer used by http_request_body in pwd, at line 1585 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	1919
Object	getenv	pwd

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1919.                                   strcpy(new->pwd, url->pwd);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=42
Status	New

The size of the buffer used by http_request_body in pwd, at line 1585 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1760	1919
Object	getenv	pwd

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1760.              if ((p = getenv("HTTP_USER_AGENT")) != NULL) {
....
1919.                                   strcpy(new->pwd, url->pwd);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=43
Status	New

The size of the buffer used by http_request_body in user, at line 1585 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	1918
Object	getenv	user

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1918.                                  strcpy(new->user, url->user);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=44
Status	New

The size of the buffer used by http_request_body in user, at line 1585 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	1918
Object	getenv	user

Code Snippet
File Name ravynos-1/http.c

Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.         if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1918.                                         strcpy(new->user, url->user);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=45
Status	New

The size of the buffer used by http_request_body in user, at line 1585 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1760	1918
Object	getenv	user

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1760.                   if ((p = getenv("HTTP_USER_AGENT")) != NULL) {
....
1918.                                         strcpy(new->user, url->user);
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=46
Status	New

The size of the buffer used by http_get_proxy in scheme, at line 1502 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	1514
Object	getenv	scheme

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
....
1514.                    strcpy(purl->scheme, SCHEME_HTTP);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=47
Status	New

The size of the buffer used by http_get_proxy in scheme, at line 1502 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	1514
Object	getenv	scheme

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
....
1514.                    strcpy(purl->scheme, SCHEME_HTTP);
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=48
Status	New

The size of the buffer used by *CRYPTO_strdup in ret, at line 27 of ravynos-1/o_str.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *CRYPTO_strdup passes to file, at line 27 of ravynos-1/o_str.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/o_str.c	ravynos-1/o_str.c
Line	27	35
Object	file	ret

Code Snippet

File Name	ravynos-1/o_str.c
Method	char *CRYPTO_strdup(const char *str, const char* file, int line)

```
....
27.  char *CRYPTO_strdup(const char *str, const char* file, int line)
....
35.          strcpy(ret, str);
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=49
Status	New

The size of the buffer used by my_popen in command, at line 67 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that my_popen passes to command, at line 67 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	67	92
Object	command	command

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
67.  my_popen(const char *command, const char *dir, pid_t *p_pid)
....
92.   strcpy(cmd2, command);
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=50
Status	New

The size of the buffer used by my_popen in command, at line 67 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that add_it_to passes to vars, at line 2641 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2641	92
Object	vars	command

Code Snippet
File Name ravynos-1/pmcstudy.c
Method add_it_to(char **vars, int cur_cnt, char *name)

```
....
2641.   add_it_to(char **vars, int cur_cnt, char *name)
```

File Name ravynos-1/pmcstudy.c
Method my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
92.    strcpy(cmd2, command);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=51
Status	New

The size of the buffer used by build_command_for_exp in forming, at line 2669 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that add_it_to passes to vars, at line 2641 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2641	2728
Object	vars	forming

Code Snippet
File Name ravynos-1/pmcstudy.c
Method add_it_to(char **vars, int cur_cnt, char *name)

```
....
2641.   add_it_to(char **vars, int cur_cnt, char *name)
```

File Name	ravynos-1/pmcstudy.c
Method	build_command_for_exp(struct expression *exp)

```
....
2728.               strcat(cmd, forming);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=52
Status	New

The size of the buffer used by build_command_for_exp in cmd, at line 2669 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that add_it_to passes to vars, at line 2641 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2641	2728
Object	vars	cmd

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	add_it_to(char **vars, int cur_cnt, char *name)

```
....
2641.   add_it_to(char **vars, int cur_cnt, char *name)
```

▼

File Name	ravynos-1/pmcstudy.c
Method	build_command_for_exp(struct expression *exp)

```
....
2728.               strcat(cmd, forming);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=53
Status	New

The size of the buffer used by filter_add in neW, at line 635 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that filter_add passes to filt, at line 635 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	635	656
Object	filt	neW

Code Snippet
File Name ravynos-1/lockstat.c
Method filter_add(char **filt, char *what, uintptr_t base, size_t size)

```
....
635.   filter_add(char **filt, char *what, uintptr_t base, size_t size)
....
656.          (void) strcat(new, c);
```

Buffer Overflow OutOfBound

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

Categories

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

Description

Buffer Overflow OutOfBound\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=90
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that { passes to g_event_info, at line 147 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	147	1295
Object	g_event_info	i

Code Snippet
File Name ravynos-1/lockstat.c
Method static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {

```
....
147.   static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {
```

▼

File Name ravynos-1/lockstat.c
Method main(int argc, char **argv)

```
....
1295.                    if (g_event_info[i].ev_type == c)
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=91
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that { passes to g_event_info, at line 147 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	147	1194
Object	g_event_info	i

Code Snippet

File Name   ravynos-1/lockstat.c

Method   static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {

```
....
147.  static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {
```

File Name   ravynos-1/lockstat.c

Method   main(int argc, char **argv)

```
....
1194.                    if (g_event_info[i].ev_type != 'E')
```

Buffer Overflow OutOfBound\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=92
Status	New

The size of the buffer used by main in g_event_info, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that { passes to g_event_info, at line 147 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	147	1302

Object	g_event_info	g_event_info

Code Snippet
File Name ravynos-1/lockstat.c
Method static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {

```
....
147.  static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {
```

File Name ravynos-1/lockstat.c

Method main(int argc, char **argv)

```
....
1302.                           if (strchr("CH", g_event_info[i].ev_type))
```

Buffer Overflow OutOfBound\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=93
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that { passes to g_event_info, at line 147 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	147	1375
Object	g_event_info	i

Code Snippet
File Name ravynos-1/lockstat.c
Method static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {

```
....
147.  static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {
```

File Name ravynos-1/lockstat.c

Method main(int argc, char **argv)

```
....
1375.              if (!events_specified && g_event_info[i].ev_type ==
'C')
```

Buffer Overflow OutOfBound\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=94
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that { passes to g_event_info, at line 147 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	147	1383
Object	g_event_info	i

Code Snippet

File Name ravynos-1/lockstat.c

Method static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {

```
....
147.  static ls_event_info_t g_event_info[LS_MAX_EVENTS] = {
```

File Name ravynos-1/lockstat.c

Method main(int argc, char **argv)

```
....
1383.            if (g_event_info[i].ev_acquire != NULL) {
```

Buffer Overflow OutOfBound\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=95
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that g_min_duration[LS_MAX_EVENTS]; passes to g_min_duration, at line 129 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	129	1195
Object	g_min_duration	i

Code Snippet

File Name ravynos-1/lockstat.c

Method	static hrtime_t g_min_duration[LS_MAX_EVENTS];

```
....
129.   static hrtime_t g_min_duration[LS_MAX_EVENTS];
```

▼

File Name	ravynos-1/lockstat.c
Method	main(int argc, char **argv)

```
....
1195.                                    g_min_duration[i] = duration;
```

Buffer Overflow OutOfBound\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=96
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that g_enabled[LS_MAX_EVENTS]; passes to g_enabled, at line 128 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	128	1296
Object	g_enabled	i

Code Snippet

File Name	ravynos-1/lockstat.c
Method	static uchar_t g_enabled[LS_MAX_EVENTS];

```
....
128.   static uchar_t g_enabled[LS_MAX_EVENTS];
```

▼

File Name	ravynos-1/lockstat.c
Method	main(int argc, char **argv)

```
....
1296.                                    g_enabled[i] = 1;
```

Buffer Overflow OutOfBound\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=97

Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that g_enabled[LS_MAX_EVENTS]; passes to g_enabled, at line 128 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	128	1262
Object	g_enabled	i

Code Snippet
File Name ravynos-1/lockstat.c
Method static uchar_t g_enabled[LS_MAX_EVENTS];

```
....
128.   static uchar_t g_enabled[LS_MAX_EVENTS];
```

File Name ravynos-1/lockstat.c

Method main(int argc, char **argv)

```
....
1262.                                 g_enabled[i] = 1;
```

Buffer Overflow OutOfBound\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=98
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that g_enabled[LS_MAX_EVENTS]; passes to g_enabled, at line 128 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	128	1303
Object	g_enabled	i

Code Snippet
File Name ravynos-1/lockstat.c
Method static uchar_t g_enabled[LS_MAX_EVENTS];

```
....
128.  static uchar_t g_enabled[LS_MAX_EVENTS];
```

File Name ravynos-1/lockstat.c

Method main(int argc, char **argv)

```
....
1303.                                g_enabled[i] = 1;
```

Buffer Overflow OutOfBound\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=99
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that g_enabled[LS_MAX_EVENTS]; passes to g_enabled, at line 128 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	128	1376
Object	g_enabled	i

Code Snippet

File Name ravynos-1/lockstat.c

Method static uchar_t g_enabled[LS_MAX_EVENTS];

```
....
128.  static uchar_t g_enabled[LS_MAX_EVENTS];
```

File Name ravynos-1/lockstat.c

Method main(int argc, char **argv)

```
....
1376.                    g_enabled[i] = 1;
```

Buffer Overflow OutOfBound\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=100
Status	New

The size of the buffer used by main in i, at line 1114 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that g_enabled[LS_MAX_EVENTS]; passes to g_enabled, at line 128 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	128	1380
Object	g_enabled	i

Code Snippet
File Name ravynos-1/lockstat.c
Method static uchar_t g_enabled[LS_MAX_EVENTS];

```
....
128.   static uchar_t g_enabled[LS_MAX_EVENTS];
```

File Name ravynos-1/lockstat.c

Method main(int argc, char **argv)

```
....
1380.              if (!g_enabled[i])
```

Buffer Overflow OutOfBound\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=101
Status	New

The size of the buffer used by test_for_a_pmc in i, at line 2568 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that my_popen passes to pdesin, at line 67 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	70	2601
Object	pdesin	i

Code Snippet
File Name ravynos-1/pmcstudy.c
Method my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
70.   int pdesin[2], pdesout[2];
```

File Name	ravynos-1/pmcstudy.c
Method	test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2601.            if (strncmp(&line[i], "ERROR", 5) == 0) {
```

Buffer Overflow OutOfBound\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=102
Status	New

The size of the buffer used by process_header in i, at line 2064 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that my_popen passes to pdesin, at line 67 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	70	2083
Object	pdesin	i

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
70.    int pdesin[2], pdesout[2];
```

File Name	ravynos-1/pmcstudy.c
Method	process_header(int idx, char *p)

```
....
2083.            if (p[i] == '/') {
```

Buffer Overflow OutOfBound\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=103
Status	New

The size of the buffer used by test_for_a_pmc in i, at line 2568 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that my_popen passes to pdesin, at line 67 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	70	2604
Object	pdesin	i

Code Snippet
File Name ravynos-1/pmcstudy.c
Method my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
70.    int pdesin[2], pdesout[2];
```

File Name ravynos-1/pmcstudy.c

Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2604.            } else if (strncmp(&line[i], resp, len) == 0) {
```

CGI Stored XSS

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

Categories

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

Description

CGI Stored XSS\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=104
Status	New

Unvalidated DB output was found in line number 2095 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2064.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2104	2075
Object	buffer	printf

Code Snippet
File Name ravynos-1/pmcstudy.c
Method build_counters_from_header(FILE *io)

```
....
2104.        if (fgets(buffer, sizeof(buffer), io) == NULL) {
```

▼

File Name	ravynos-1/pmcstudy.c
Method	process_header(int idx, char *p)

```
....
2075.              printf("Check -- invalid header no s/ in %s\n",
```

CGI Stored XSS\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=105
Status	New

Unvalidated DB output was found in line number 2334 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2787.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2510	2793
Object	linebuf	printf

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	get_cpuid_set(void)

```
....
2510.        while (fgets(linebuf, sizeof(linebuf), io) != NULL) {
```

▼

File Name	ravynos-1/pmcstudy.c
Method	list_all(void)

```
....
2793.              cnt = printf("%s", valid_pmcs[i]);
```

CGI Stored XSS\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=106
Status	New

Unvalidated DB output was found in line number 2334 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2775.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2510	2781
Object	linebuf	printf

Code Snippet

File Name ravynos-1/pmcstudy.c

Method get_cpuid_set(void)

```
....
2510.        while (fgets(linebuf, sizeof(linebuf), io) != NULL) {
```

File Name ravynos-1/pmcstudy.c

Method run_tests(void)

```
....
2781.                lenout = printf("%s", valid_pmcs[i]);
```

CGI Stored XSS\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=107
Status	New

Unvalidated DB output was found in line number 2568 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2568.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2591	2602
Object	line	printf

Code Snippet

File Name ravynos-1/pmcstudy.c

Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2591.        if (fgets(line, sizeof(line), io) == NULL) {
....
2602.                    printf("Failed %s\n", line);
```

CGI Stored XSS\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=108
Status	New

Unvalidated DB output was found in line number 2568 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2568.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2591	2627
Object	line	printf

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2591.           if (fgets(line, sizeof(line), io) == NULL) {
....
2627.                               printf("%s", &line[j]);
```

CGI Stored XSS\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=109
Status	New

Unvalidated DB output was found in line number 2568 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2568.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2591	2634
Object	line	printf

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2591.           if (fgets(line, sizeof(line), io) == NULL) {
....
2634.           printf("Failed -- '%s' not '%s'\n", line, resp);
```

CGI Stored XSS\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=110
Status	New

Unvalidated DB output was found in line number 2568 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2568.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2607	2602
Object	line	printf

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2607.                       if (fgets(line, sizeof(line), io) == NULL) {
....
2602.                       printf("Failed %s\n", line);
```

CGI Stored XSS\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=111
Status	New

Unvalidated DB output was found in line number 2568 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2568.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2607	2634
Object	line	printf

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2607.                       if (fgets(line, sizeof(line), io) == NULL) {
....
2634.           printf("Failed -- '%s' not '%s'\n", line, resp);
```

CGI Stored XSS\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=112
Status	New

Unvalidated DB output was found in line number 2568 in ravynos-1/pmcstudy.c file. A possible XSS exploitation was found in printf at line number 2568.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2607	2627
Object	line	printf

Code Snippet
File Name ravynos-1/pmcstudy.c
Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2607.                   if (fgets(line, sizeof(line), io) == NULL) {
....
2627.                        printf("%s", &line[j]);
```

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=1070095&projectid=70085&pathid=1
Status	New

The size of the buffer used by my_popen in argv, at line 67 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that build_command_for_exp passes to "/usr/sbin/pmcstat -w 1", at line 2669 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2724	95
Object	"/usr/sbin/pmcstat -w 1"	argv

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	build_command_for_exp(struct expression *exp)

```
....
2724.        strcpy(cmd, "/usr/sbin/pmcstat -w 1");
```

File Name	ravynos-1/pmcstudy.c
Method	my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
95.    argv[2] = cmd2;
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=2
Status	New

The size of the buffer used by my_popen in argv, at line 67 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that build_command_for_exp passes to " -s %s", at line 2669 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2727	95
Object	" -s %s"	argv

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	build_command_for_exp(struct expression *exp)

```
....
2727.            sprintf(forming, " -s %s", vars[i]);
```

File Name	ravynos-1/pmcstudy.c
Method	my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
95.    argv[2] = cmd2;
```

Buffer Overflow LongString\Path 3:

Severity	High

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=3
Status	New

The size of the buffer used by my_popen in argv, at line 67 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_cpuid_set passes to "/usr/sbin/pmccontrol - ", at line 2334 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2497	95
Object	"/usr/sbin/pmccontrol - "	argv

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	get_cpuid_set(void)

```
....
2497.        io = my_popen("/usr/sbin/pmccontrol -L", "r",
&pid_of_command);
```

▼

File Name	ravynos-1/pmcstudy.c
Method	my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
95.    argv[2] = cmd2;
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=4
Status	New

The size of the buffer used by my_popen in argv, at line 67 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_for_a_pmc passes to "/usr/sbin/pmcstat -w .25 -c 0 -s %s", at line 2568 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2583	95
Object	"/usr/sbin/pmcstat -w .25 -c 0 -s %s"	argv

Code Snippet

File Name	ravynos-1/pmcstudy.c

Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2583.        sprintf(my_command, "/usr/sbin/pmcstat -w .25 -c 0 -s %s",
pmc);
```

File Name ravynos-1/pmcstudy.c

Method my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
95.    argv[2] = cmd2;
```

Buffer Overflow boundedcpy

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

Categories

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

Description

Buffer Overflow boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=36
Status	New

The size parameter BinaryExpr in line 223 in file ravynos-1/phttpget.c is influenced by the user input argv in line 293 in file ravynos-1/phttpget.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	293	232
Object	argv	BinaryExpr

Code Snippet
File Name ravynos-1/phttpget.c
Method main(int argc, char *argv[])

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

File Name ravynos-1/phttpget.c

Method readln(int sd, char * resbuf, int * resbuflen, int * resbufpos)

```
....
232.                        *resbuflen - *resbufpos);
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=37
Status	New

The size parameter BinaryExpr in line 223 in file ravynos-1/phttpget.c is influenced by the user input BinaryExpr in line 223 in file ravynos-1/phttpget.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	242	232
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name ravynos-1/phttpget.c

Method readln(int sd, char * resbuf, int * resbuflen, int * resbufpos)

```
....
242.                  len = recv(sd, resbuf + *resbuflen, BUFSIZ -
*resbuflen, 0);
....
232.                        *resbuflen - *resbufpos);
```

Buffer Overflow boundedcpy\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=38
Status	New

The size parameter BinaryExpr in line 223 in file ravynos-1/phttpget.c is influenced by the user input resbuf in line 255 in file ravynos-1/phttpget.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	276	232
Object	resbuf	BinaryExpr

Code Snippet

File Name	ravynos-1/phttpget.c
Method	copybytes(int sd, int fd, off_t copylen, char * resbuf, int * resbuflen,

```
....
276.                len = recv(sd, resbuf, BUFSIZ, 0);
```

File Name	ravynos-1/phttpget.c
Method	readln(int sd, char * resbuf, int * resbuflen, int * resbufpos)

```
....
232.                          *resbuflen - *resbufpos);
```

Buffer Overflow boundedcpy\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=39
Status	New

The size parameter len in line 2021 in file ravynos-1/test_x509.c is influenced by the user input argv in line 2021 in file ravynos-1/test_x509.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	2021	2050
Object	argv	len

Code Snippet

File Name	ravynos-1/test_x509.c
Method	main(int argc, const char *argv[])

```
....
2021.  main(int argc, const char *argv[])
....
2050.                          memcpy(dn, arg, len);
```

Command Injection

Query Path:
CPP\Cx\CPP High Risk\Command 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

Command Injection\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=113
Status	New

The application's main method calls an OS (shell) command with execvp, at line 1114 of ravynos-1/lockstat.c, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, argv, which is retrieved by the application in the main method, at line 1114 of ravynos-1/lockstat.c.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1114	1476
Object	argv	execvp

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

```
....
1114.   main(int argc, char **argv)
....
1476.               (void) execvp(argv[0], &argv[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=1070095&projectid=70085&pathid=490
Status	New

The dangerous function, memcpy, was found in use at line 2355 in ravynos-1/archive_read_support_format_lha.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	2494	2494
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lzh_decode_blocks(struct lzh_stream *strm, int last)

```
....
2494.                                   memcpy(w_buff + w_pos,
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=491
Status	New

The dangerous function, memcpy, was found in use at line 2702 in ravynos-1/archive_read_support_format_lha.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	2799	2799
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lzh_make_huffman_table(struct huffman *hf)

```
....
2799.                                   memcpy(&p[cnt], pc,
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=492
Status	New

The dangerous function, memcpy, was found in use at line 2702 in ravynos-1/archive_read_support_format_lha.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	2804	2804
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lzh_make_huffman_table(struct huffman *hf)

```
....
2804.                                                    memcpy(&p[cnt], pc,
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=493
Status	New

The dangerous function, memcpy, was found in use at line 2702 in ravynos-1/archive_read_support_format_lha.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	2809	2809
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lzh_make_huffman_table(struct huffman *hf)

```
....
2809.                                            memcpy(p, pc, cnt *
sizeof(uint16_t));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=494
Status	New

The dangerous function, memcpy, was found in use at line 2084 in ravynos-1/archive_read_support_format_mtree.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	2120	2120
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method readline(struct archive_read *a, struct mtree *mtree, char **start,

```
....
2120.              memcpy(mtree->line.s + total_size, t, bytes_read);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=495
Status	New

The dangerous function, memcpy, was found in use at line 813 in ravynos-1/archive_read_support_format_mtree.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	827	827
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method add_option(struct archive_read *a, struct mtree_option **global,

```
....
827.        memcpy(opt->value, value, len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=496
Status	New

The dangerous function, memcpy, was found in use at line 919 in ravynos-1/archive_read_support_format_mtree.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	987	987
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	process_add_entry(struct archive_read *a, struct mtree *mtree,

```
....
987.          memcpy(entry->name, name, name_len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=497
Status	New

The dangerous function, memcpy, was found in use at line 676 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	696	696
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	lzss_emit_match(struct rar *rar, int offset, int length)

```
....
696.          memcpy(d, s, l);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=498

Status	New

The dangerous function, memcpy, was found in use at line 907 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	983	983
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=499
Status	New

The dangerous function, memcpy, was found in use at line 907 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	984	984
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
984.        memcpy(rar->reserved2, p + 7 + sizeof(rar->reserved1),
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=500
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1395	1395
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1395.     memcpy(&rar_header, p, sizeof(rar_header));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=501
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1448	1448
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1448.     memcpy(&file_header, p, sizeof(file_header));
```

Dangerous Functions\Path 13:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=502
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1472	1472
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1472.       memcpy(packed_size, file_header.pack_size, 4);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=503
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1473	1473
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1473.       memcpy(packed_size + 4, p, 4); /* High pack size */
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=504
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1475	1475
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1475.       memcpy(unp_size, file_header.unp_size, 4);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=505
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1476	1476
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1476.       memcpy(unp_size + 4, p, 4); /* High unpack size */
```

Dangerous Functions\Path 17:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=506
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1529	1529
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1529.     memcpy(filename, p, filename_size);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=507
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1683	1683
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1683.     memcpy(rar->filename_save, rar->filename, filename_size + 1);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=508
Status	New

The dangerous function, memcpy, was found in use at line 1358 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1706	1706
Object	memcpy	memcpy

Code Snippet

File Name ravynos-1/archive_read_support_format_rar.c

Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1706.       memcpy(rar->salt, p, 8);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=509
Status	New

The dangerous function, memcpy, was found in use at line 3069 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3083	3083
Object	memcpy	memcpy

Code Snippet

File Name ravynos-1/archive_read_support_format_rar.c

Method copy_from_lzss_window(struct archive_read *a, void *buffer,

```
....
3083.       memcpy(buffer, &rar->lzss.window[windowoffs], firstpart);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=510
Status	New

The dangerous function, memcpy, was found in use at line 3069 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3084	3084
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method copy_from_lzss_window(struct archive_read *a, void *buffer,

```
....
3084.       memcpy(buffer, &rar->lzss.window[0], length - firstpart);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=511
Status	New

The dangerous function, memcpy, was found in use at line 3069 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3086	3086
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method copy_from_lzss_window(struct archive_read *a, void *buffer,

```
....
3086.       memcpy(buffer, &rar->lzss.window[windowoffs], length);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=512
Status	New

The dangerous function, memcpy, was found in use at line 3092 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3110	3110
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method copy_from_lzss_window_to_unp(struct archive_read *a, const void **buffer,

```
....
3110.       memcpy(&rar->unp_buffer[rar->unp_offset], &rar-
>lzss.window[windowoffs],
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=513
Status	New

The dangerous function, memcpy, was found in use at line 3092 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3120	3120
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method copy_from_lzss_window_to_unp(struct archive_read *a, const void **buffer,

```
....
3120.          memcpy(&rar->unp_buffer[rar->unp_offset],
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=514
Status	New

The dangerous function, memcpy, was found in use at line 3092 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3122	3122
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method copy_from_lzss_window_to_unp(struct archive_read *a, const void **buffer,

```
....
3122.          memcpy(&rar->unp_buffer[rar->unp_offset + firstpart],
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=515
Status	New

The dangerous function, memcpy, was found in use at line 3092 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3125	3125
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c

Method	copy_from_lzss_window_to_unp(struct archive_read *a, const void **buffer,

```
....
3125.          memcpy(&rar->unp_buffer[rar->unp_offset],
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=516
Status	New

The dangerous function, memcpy, was found in use at line 3313 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3326	3326
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3326.       memcpy(filter->globaldata, globaldata, globaldatalen);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=517
Status	New

The dangerous function, memcpy, was found in use at line 3313 in ravynos-1/archive_read_support_format_rar.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3328	3328
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3328.      memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=518
Status	New

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

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

Code Snippet

File Name	ravynos-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 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=519
Status	New

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

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

Code Snippet

File Name	ravynos-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 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=520
Status	New

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

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

Code Snippet

File Name	ravynos-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 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=521
Status	New

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

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

Code Snippet

File Name	ravynos-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 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=522
Status	New

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

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

Code Snippet

File Name	ravynos-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 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=523
Status	New

The dangerous function, memcpy, was found in use at line 828 in ravynos-1/b_print.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c
Line	852	852
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/b_print.c
Method	doapr_outch(char **sbuffer,

```
....
852.                        memcpy(*buffer, *sbuffer, *currlen);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=524
Status	New

The dangerous function, memcpy, was found in use at line 85 in ravynos-1/cap_sendmsg.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/cap_sendmsg.c	ravynos-1/cap_sendmsg.c
Line	120	120
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/cap_sendmsg.c
Method sendpacket(int sock, struct sockaddr_in6 *dst, uint32_t ifindex, int hoplimit,

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

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=525
Status	New

The dangerous function, memcpy, was found in use at line 1253 in ravynos-1/channels.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	1314	1314
Object	memcpy	memcpy

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

```
....
1314.        memcpy(ucp + 12 + ((proto_len + 3) & ~3),
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=526
Status	New

The dangerous function, memcpy, was found in use at line 1509 in ravynos-1/channels.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	1561	1561
Object	memcpy	memcpy

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

```
....
1561.        memcpy(&s5_req, p, sizeof(s5_req));
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=527
Status	New

The dangerous function, memcpy, was found in use at line 170 in ravynos-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	ravynos-1/cms_enc.c	ravynos-1/cms_enc.c
Line	180	180
Object	memcpy	memcpy

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

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

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=528
Status	New

The dangerous function, memcpy, was found in use at line 1115 in ravynos-1/cxgbetool.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	1299	1299
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/cxgbetool.c
Method set_filter(uint32_t idx, int argc, const char *argv[], int hash)

```
....
1299.                       memcpy(t.fs.dmac, daddr, ETHER_ADDR_LEN);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=529
Status	New

The dangerous function, memcpy, was found in use at line 1115 in ravynos-1/cxgbetool.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	1310	1310
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/cxgbetool.c
Method set_filter(uint32_t idx, int argc, const char *argv[], int hash)

```
....
1310.                   memcpy(t.fs.smac, saddr, ETHER_ADDR_LEN);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=530
Status	New

The dangerous function, memcpy, was found in use at line 769 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	790	790
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/dp_rx.c
Method static void ath11k_dp_rx_tid_del_func(struct ath11k_dp *dp, void *ctx,

```
....
790.          memcpy(&elem->data, rx_tid, sizeof(*rx_tid));
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=531
Status	New

The dangerous function, memcpy, was found in use at line 1249 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1267	1267
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/dp_rx.c
Method static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1267.                memcpy((void *)&ppdu_info->ppdu_stats.common, ptr,
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=532
Status	New

The dangerous function, memcpy, was found in use at line 1249 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1289	1289
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/dp_rx.c
Method static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1289.                memcpy((void *)&user_stats->rate, ptr,
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=533
Status	New

The dangerous function, memcpy, was found in use at line 1249 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1312	1312
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/dp_rx.c
Method static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1312.                memcpy((void *)&user_stats->cmpltn_cmn, ptr,
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=534
Status	New

The dangerous function, memcpy, was found in use at line 1249 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1337	1337
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/dp_rx.c
Method	static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1337.                memcpy((void *)&user_stats->ack_ba, ptr,
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=535
Status	New

The dangerous function, memcpy, was found in use at line 1395 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1523	1523
Object	memcpy	memcpy

Code Snippet

File Name	ravynos-1/dp_rx.c
Method	ath11k_update_per_peer_tx_stats(struct ath11k *ar,

```
....
1523.       memcpy(&arsta->last_txrate, &arsta->txrate, sizeof(struct
rate_info));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=536
Status	New

The dangerous function, memcpy, was found in use at line 1979 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	2030	2030
Object	memcpy	memcpy

Code Snippet

File Name ravynos-1/dp_rx.c

Method static void ath11k_dp_rx_h_undecap_nwifi(struct ath11k *ar,

```
....
2030.           memcpy(decap_hdr, (uint8_t *)hdr, hdr_len);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=537
Status	New

The dangerous function, memcpy, was found in use at line 1979 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	2034	2034
Object	memcpy	memcpy

Code Snippet

File Name ravynos-1/dp_rx.c

Method static void ath11k_dp_rx_h_undecap_nwifi(struct ath11k *ar,

```
....
2034.              memcpy(skb_push(msdu,
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=538
Status	New

The dangerous function, memcpy, was found in use at line 1979 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	2045	2045
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/dp_rx.c
Method static void ath11k_dp_rx_h_undecap_nwifi(struct ath11k *ar,

```
....
2045.              memcpy(skb_push(msdu,
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=539
Status	New

The dangerous function, memcpy, was found in use at line 1979 in ravynos-1/dp_rx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	2048	2048
Object	memcpy	memcpy

Code Snippet
File Name ravynos-1/dp_rx.c
Method static void ath11k_dp_rx_h_undecap_nwifi(struct ath11k *ar,

```
....
2048.           memcpy(skb_push(msdu, hdr_len), decap_hdr, hdr_len);
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=128
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	983	983
Object	->	->

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
983.        memcpy(rar->reserved1, p + 7, sizeof(rar->reserved1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=129
Status	New

The size of the buffer used by archive_read_format_rar_read_header in ->, at line 907 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that archive_read_format_rar_read_header passes to ->, at line 907 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	985	985
Object	->	->

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method archive_read_format_rar_read_header(struct archive_read *a,

```
....
985.                    sizeof(rar->reserved2));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=130
Status	New

The size of the buffer used by create_filter in ->, at line 3313 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that create_filter passes to ->, at line 3313 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3328	3328
Object	->	->

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3328.       memcpy(filter->initialregisters, registers, sizeof(filter-
>initialregisters));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=131
Status	New

The size of the buffer used by rrset_add_rr in old, at line 795 of ravynos-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 ravynos-1/authzone.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	809	809
Object	old	old

Code Snippet

File Name	ravynos-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 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=132
Status	New

The size of the buffer used by rrset_moveover_rrsigs in packed_rrset_data, at line 936 of ravynos-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 ravynos-1/authzone.c, to overwrite the target buffer.

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

Code Snippet

File Name	ravynos-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 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=133
Status	New

The size of the buffer used by rrset_moveover_rrsigs in packed_rrset_data, at line 936 of ravynos-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 ravynos-1/authzone.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1027	1027
Object	packed_rrset_data	packed_rrset_data

Code Snippet
File Name ravynos-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 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=134
Status	New

The size of the buffer used by sendpacket in int, at line 85 of ravynos-1/cap_sendmsg.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sendpacket passes to int, at line 85 of ravynos-1/cap_sendmsg.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cap_sendmsg.c	ravynos-1/cap_sendmsg.c
Line	120	120
Object	int	int

Code Snippet
File Name ravynos-1/cap_sendmsg.c
Method sendpacket(int sock, struct sockaddr_in6 *dst, uint32_t ifindex, int hoplimit,

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

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=135
Status	New

The size of the buffer used by ath11k_dp_rx_tid_del_func in rx_tid, at line 769 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_dp_rx_tid_del_func passes to rx_tid, at line 769 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	790	790
Object	rx_tid	rx_tid

Code Snippet

File Name	ravynos-1/dp_rx.c
Method	static void ath11k_dp_rx_tid_del_func(struct ath11k_dp *dp, void *ctx,

```
....
790.        memcpy(&elem->data, rx_tid, sizeof(*rx_tid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=136
Status	New

The size of the buffer used by ath11k_htt_tlv_ppdu_stats_parse in htt_ppdu_stats_common, at line 1249 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_htt_tlv_ppdu_stats_parse passes to htt_ppdu_stats_common, at line 1249 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1268	1268
Object	htt_ppdu_stats_common	htt_ppdu_stats_common

Code Snippet

File Name	ravynos-1/dp_rx.c
Method	static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1268.                   sizeof(struct htt_ppdu_stats_common));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=137
Status	New

The size of the buffer used by ath11k_htt_tlv_ppdu_stats_parse in htt_ppdu_stats_user_rate, at line 1249 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_htt_tlv_ppdu_stats_parse passes to htt_ppdu_stats_user_rate, at line 1249 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1290	1290
Object	htt_ppdu_stats_user_rate	htt_ppdu_stats_user_rate

Code Snippet
File Name ravynos-1/dp_rx.c
Method static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1290.                        sizeof(struct htt_ppdu_stats_user_rate));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=138
Status	New

The size of the buffer used by ath11k_htt_tlv_ppdu_stats_parse in htt_ppdu_stats_usr_cmpltn_cmn, at line 1249 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_htt_tlv_ppdu_stats_parse passes to htt_ppdu_stats_usr_cmpltn_cmn, at line 1249 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1313	1313
Object	htt_ppdu_stats_usr_cmpltn_cmn	htt_ppdu_stats_usr_cmpltn_cmn

Code Snippet
File Name ravynos-1/dp_rx.c
Method static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1313.                        sizeof(struct htt_ppdu_stats_usr_cmpltn_cmn));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=139
Status	New

The size of the buffer used by ath11k_htt_tlv_ppdu_stats_parse in htt_ppdu_stats_usr_cmpltn_ack_ba_status, at line 1249 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_htt_tlv_ppdu_stats_parse passes to htt_ppdu_stats_usr_cmpltn_ack_ba_status, at line 1249 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1338	1338
Object	htt_ppdu_stats_usr_cmpltn_ack_ba_status	htt_ppdu_stats_usr_cmpltn_ack_ba_status

Code Snippet

File Name	ravynos-1/dp_rx.c
Method	static int ath11k_htt_tlv_ppdu_stats_parse(struct ath11k_base *ab,

```
....
1338.                    sizeof(struct
htt_ppdu_stats_usr_cmpltn_ack_ba_status));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=140
Status	New

The size of the buffer used by ath11k_update_per_peer_tx_stats in rate_info, at line 1395 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_update_per_peer_tx_stats passes to rate_info, at line 1395 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1523	1523
Object	rate_info	rate_info

Code Snippet

File Name	ravynos-1/dp_rx.c
Method	ath11k_update_per_peer_tx_stats(struct ath11k *ar,

```
....
1523.      memcpy(&arsta->last_txrate, &arsta->txrate, sizeof(struct
rate_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=141
Status	New

The size of the buffer used by ath11k_dp_rx_h_undecap_eth in ath11k_dp_rfc1042_hdr, at line 2161 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_dp_rx_h_undecap_eth passes to ath11k_dp_rfc1042_hdr, at line 2161 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	2186	2186
Object	ath11k_dp_rfc1042_hdr	ath11k_dp_rfc1042_hdr

Code Snippet
File Name ravynos-1/dp_rx.c
Method static void ath11k_dp_rx_h_undecap_eth(struct ath11k *ar,

```
....
2186.                sizeof(struct ath11k_dp_rfc1042_hdr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=142
Status	New

The size of the buffer used by ath11k_dp_rx_deliver_msdu in known, at line 2477 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_dp_rx_deliver_msdu passes to known, at line 2477 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	2499	2499
Object	known	known

Code Snippet
File Name ravynos-1/dp_rx.c
Method static void ath11k_dp_rx_deliver_msdu(struct ath11k *ar, struct napi_struct *napi,

```
....
2499.               memcpy(he, &known, sizeof(known));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=143
Status	New

The size of the buffer used by ath11k_dp_rx_mon_merg_msdus in __le16, at line 4873 of ravynos-1/dp_rx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ath11k_dp_rx_mon_merg_msdus passes to __le16, at line 4873 of ravynos-1/dp_rx.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	4951	4951
Object	__le16	__le16

Code Snippet
File Name ravynos-1/dp_rx.c
Method ath11k_dp_rx_mon_merg_msdus(struct ath11k *ar,

```
....
4951.                                    (u8 *)&qos_field, sizeof(__le16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=144
Status	New

The size of the buffer used by fwctl_response in uint32_t, at line 399 of ravynos-1/fwctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fwctl_response passes to uint32_t, at line 399 of ravynos-1/fwctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/fwctl.c	ravynos-1/fwctl.c
Line	427	427
Object	uint32_t	uint32_t

Code Snippet
File Name ravynos-1/fwctl.c
Method fwctl_response(uint32_t *retval)

```
....
427.                    memcpy(retval, dp, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=145
Status	New

The size of the buffer used by imsg_get in ->, at line 126 of ravynos-1/imsg.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that imsg_get passes to ->, at line 126 of ravynos-1/imsg.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/imsg.c	ravynos-1/imsg.c
Line	135	135
Object	->	->

Code Snippet
File Name ravynos-1/imsg.c
Method imsg_get(struct imsgbuf *ibuf, struct imsg *imsg)

```
....
135.         memcpy(&imsg->hdr, ibuf->r.buf, sizeof(imsg->hdr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=146
Status	New

The size of the buffer used by mrsas_get_seq_num in mrsas_evt_log_info, at line 566 of ravynos-1/mrsas.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mrsas_get_seq_num passes to mrsas_evt_log_info, at line 566 of ravynos-1/mrsas.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	607	607
Object	mrsas_evt_log_info	mrsas_evt_log_info

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_get_seq_num(struct mrsas_softc *sc,

```
....
607.         memcpy(eli, sc->el_info_mem, sizeof(struct
mrsas_evt_log_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=147
Status	New

The size of the buffer used by mrsas_get_ctrl_info in mrsas_ctrl_info, at line 3607 of ravynos-1/mrsas.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mrsas_get_ctrl_info passes to mrsas_ctrl_info, at line 3607 of ravynos-1/mrsas.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	3648	3648
Object	mrsas_ctrl_info	mrsas_ctrl_info

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_get_ctrl_info(struct mrsas_softc *sc)

```
....
3648.            memcpy(sc->ctrl_info, sc->ctlr_info_mem, sizeof(struct
mrsas_ctrl_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=148
Status	New

The size of the buffer used by mrsas_get_pd_list in ->, at line 4560 of ravynos-1/mrsas.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mrsas_get_pd_list passes to ->, at line 4560 of ravynos-1/mrsas.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	4645	4645
Object	->	->

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_get_pd_list(struct mrsas_softc *sc)

```
....
4645.            memcpy(sc->pd_list, sc->local_pd_list, sizeof(sc-
>local_pd_list));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=149
Status	New

The size of the buffer used by decode_udp_ip_header in ->, at line 165 of ravynos-1/packet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_udp_ip_header passes to ->, at line 165 of ravynos-1/packet.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/packet.c	ravynos-1/packet.c
Line	248	248
Object	->	->

Code Snippet
File Name   ravynos-1/packet.c
Method   decode_udp_ip_header(unsigned char *buf, int bufix, struct sockaddr_in *from,

```
....
248.         memcpy(&from->sin_port, &udp->uh_sport, sizeof(udp-
>uh_sport));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=150
Status	New

The size of the buffer used by assemble_hw_header in Namespace870111211, at line 94 of ravynos-1/packet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that assemble_hw_header passes to Namespace870111211, at line 94 of ravynos-1/packet.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/packet.c	ravynos-1/packet.c
Line	102	102
Object	Namespace870111211	Namespace870111211

Code Snippet
File Name   ravynos-1/packet.c
Method   assemble_hw_header(struct interface_info *interface, unsigned char *buf,

```
....
102.                   sizeof(eh.ether_shost));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=151
Status	New

The size of the buffer used by assemble_udp_ip_header in ip, at line 113 of ravynos-1/packet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that assemble_udp_ip_header passes to ip, at line 113 of ravynos-1/packet.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/packet.c	ravynos-1/packet.c
Line	132	132
Object	ip	ip

Code Snippet
File Name ravynos-1/packet.c
Method assemble_udp_ip_header(unsigned char *buf, int *bufix, u_int32_t from,

```
....
132.        memcpy(&buf[*bufix], &ip, sizeof(ip));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=152
Status	New

The size of the buffer used by assemble_udp_ip_header in udp, at line 113 of ravynos-1/packet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that assemble_udp_ip_header passes to udp, at line 113 of ravynos-1/packet.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/packet.c	ravynos-1/packet.c
Line	145	145
Object	udp	udp

Code Snippet
File Name ravynos-1/packet.c
Method assemble_udp_ip_header(unsigned char *buf, int *bufix, u_int32_t from,

```
....
145.        memcpy(&buf[*bufix], &udp, sizeof(udp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=153
Status	New

The size of the buffer used by decode_hw_header in Namespace870111211, at line 150 of ravynos-1/packet.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_hw_header passes to Namespace870111211, at line 150 of ravynos-1/packet.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/packet.c	ravynos-1/packet.c
Line	156	156
Object	Namespace870111211	Namespace870111211

Code Snippet
File Name ravynos-1/packet.c
Method decode_hw_header(unsigned char *buf, int bufix, struct hardware *from)

```
....
156.        memcpy(from->haddr, eh.ether_shost, sizeof(eh.ether_shost));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=154
Status	New

The size of the buffer used by on_write_request_process in timeval, at line 398 of ravynos-1/query.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that on_write_request_process passes to timeval, at line 398 of ravynos-1/query.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/query.c	ravynos-1/query.c
Line	456	456
Object	timeval	timeval

Code Snippet
File Name ravynos-1/query.c
Method on_write_request_process(struct query_state *qstate)

```
....
456.                           sizeof(struct timeval));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=155
Status	New

The size of the buffer used by on_negative_write_request_process in timeval, at line 471 of ravynos-1/query.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that on_negative_write_request_process passes to timeval, at line 471 of ravynos-1/query.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/query.c	ravynos-1/query.c
Line	537	537
Object	timeval	timeval

Code Snippet
File Name ravynos-1/query.c
Method on_negative_write_request_process(struct query_state *qstate)

```
....
537.                          sizeof(struct timeval));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=156
Status	New

The size of the buffer used by on_read_request_process in timeval, at line 660 of ravynos-1/query.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that on_read_request_process passes to timeval, at line 660 of ravynos-1/query.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/query.c	ravynos-1/query.c
Line	816	816
Object	timeval	timeval

Code Snippet
File Name ravynos-1/query.c
Method on_read_request_process(struct query_state *qstate)

```
....
816.                          sizeof(struct timeval));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=157
Status	New

The size of the buffer used by sctp_connectx in sockaddr_in, at line 104 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_connectx passes to sockaddr_in, at line 104 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	134	134
Object	sockaddr_in	sockaddr_in

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_connectx(int sd, const struct sockaddr *addrs, int addrcnt,

```
....
134.                    memcpy(cpto, at, sizeof(struct sockaddr_in));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=158
Status	New

The size of the buffer used by sctp_connectx in sockaddr_in6, at line 104 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_connectx passes to sockaddr_in6, at line 104 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	149	149
Object	sockaddr_in6	sockaddr_in6

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_connectx(int sd, const struct sockaddr *addrs, int addrcnt,

```
....
149.                         memcpy(cpto, at, sizeof(struct
sockaddr_in6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=159
Status	New

The size of the buffer used by sctp_recvv in sctp_rcvinfo, at line 877 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_recvv passes to sctp_rcvinfo, at line 877 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	954	954
Object	sctp_rcvinfo	sctp_rcvinfo

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_recvv(int sd,

```
....
954.                    memcpy(info, rcvinfo, sizeof(struct
sctp_rcvinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=160
Status	New

The size of the buffer used by sctp_recvv in sctp_nxtinfo, at line 877 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_recvv passes to sctp_nxtinfo, at line 877 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	960	960
Object	sctp_nxtinfo	sctp_nxtinfo

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_recvv(int sd,

```
....
960.                    memcpy(info, nxtinfo, sizeof(struct
sctp_nxtinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=161
Status	New

The size of the buffer used by sctp_sendv in sctp_sndinfo, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to sctp_sndinfo, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1027	1027
Object	sctp_sndinfo	sctp_sndinfo

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_sendv(int sd,

```
....
1027.           memcpy(CMSG_DATA(cmsg), info, sizeof(struct
sctp_sndinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=162
Status	New

The size of the buffer used by sctp_sendv in sctp_prinfo, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to sctp_prinfo, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1041	1041
Object	sctp_prinfo	sctp_prinfo

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_sendv(int sd,

```
....
1041.           memcpy(CMSG_DATA(cmsg), info, sizeof(struct
sctp_prinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=163
Status	New

The size of the buffer used by sctp_sendv in sctp_authinfo, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to sctp_authinfo, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1054	1054
Object	sctp_authinfo	sctp_authinfo

Code Snippet

File Name	ravynos-1/sctp_sys_calls.c
Method	sctp_sendv(int sd,

```
....
1054.             memcpy(CMSG_DATA(cmsg), info, sizeof(struct 
sctp_authinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=164
Status	New

The size of the buffer used by sctp_sendv in sctp_sndinfo, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to sctp_sndinfo, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1069	1069
Object	sctp_sndinfo	sctp_sndinfo

Code Snippet

File Name	ravynos-1/sctp_sys_calls.c
Method	sctp_sendv(int sd,

```
....
1069.                   memcpy(CMSG_DATA(cmsg), &spa_info-
>sendv_sndinfo, sizeof(struct sctp_sndinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=165
Status	New

The size of the buffer used by sctp_sendv in sctp_prinfo, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to sctp_prinfo, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1078	1078
Object	sctp_prinfo	sctp_prinfo

Code Snippet

File Name	ravynos-1/sctp_sys_calls.c
Method	sctp_sendv(int sd,

```
....
1078.                     memcpy(CMSG_DATA(cmsg), &spa_info->sendv_prinfo,
sizeof(struct sctp_prinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=166
Status	New

The size of the buffer used by sctp_sendv in sctp_authinfo, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to sctp_authinfo, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1086	1086
Object	sctp_authinfo	sctp_authinfo

Code Snippet

File Name	ravynos-1/sctp_sys_calls.c
Method	sctp_sendv(int sd,

```
....
1086.                     memcpy(CMSG_DATA(cmsg), &spa_info-
>sendv_authinfo, sizeof(struct sctp_authinfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=167

Status	New

The size of the buffer used by sctp_sendv in in_addr, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to in_addr, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1117	1117
Object	in_addr	in_addr

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_sendv(int sd,

```
....
1117.                                   memcpy(CMSG_DATA(cmsg), &addr_in-
>sin_addr, sizeof(struct in_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=168
Status	New

The size of the buffer used by sctp_sendv in in6_addr, at line 970 of ravynos-1/sctp_sys_calls.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sctp_sendv passes to in6_addr, at line 970 of ravynos-1/sctp_sys_calls.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	1142	1142
Object	in6_addr	in6_addr

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_sendv(int sd,

```
....
1142.                                   memcpy(CMSG_DATA(cmsg), &addr_in6-
>sin6_addr, sizeof(struct in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=169
Status	New

The size of the buffer used by xgbe_set_rss_hash_key in ->, at line 411 of ravynos-1/xgbe-dev.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xgbe_set_rss_hash_key passes to ->, at line 411 of ravynos-1/xgbe-dev.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/xgbe-dev.c	ravynos-1/xgbe-dev.c
Line	413	413
Object	->	->

Code Snippet

File Name	ravynos-1/xgbe-dev.c
Method	xgbe_set_rss_hash_key(struct xgbe_prv_data *pdata, const uint8_t *key)

```
....
413.        memcpy(pdata->rss_key, key, sizeof(pdata->rss_key));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=170
Status	New

The size of the buffer used by lzh_read_blocks in Namespace462304372, at line 2120 of ravynos-1/archive_read_support_format_lha.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lzh_read_blocks passes to Namespace462304372, at line 2120 of ravynos-1/archive_read_support_format_lha.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	2206	2206
Object	Namespace462304372	Namespace462304372

Code Snippet

File Name	ravynos-1/archive_read_support_format_lha.c
Method	lzh_read_blocks(struct lzh_stream *strm, int last)

```
....
2206.                   memset(ds->pt.freq, 0, sizeof(ds->pt.freq));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=171
Status	New

The size of the buffer used by lzh_read_blocks in Namespace462304372, at line 2120 of ravynos-1/archive_read_support_format_lha.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lzh_read_blocks passes to Namespace462304372, at line 2120 of ravynos-1/archive_read_support_format_lha.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	2283	2283
Object	Namespace462304372	Namespace462304372

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lzh_read_blocks(struct lzh_stream *strm, int last)

```
....
2283.                           memset(ds->lt.freq, 0, sizeof(ds->lt.freq));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=172
Status	New

The size of the buffer used by read_header in ->, at line 1358 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_header passes to ->, at line 1358 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1416	1416
Object	->	->

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1416.       memset(&rar->salt, 0, sizeof(rar->salt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=173

Status	New

The size of the buffer used by read_header in ->, at line 1358 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_header passes to ->, at line 1358 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1763	1763
Object	->	->

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1763.     memset(rar->lengthtable, 0, sizeof(rar->lengthtable));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=174
Status	New

The size of the buffer used by parse_codes in ->, at line 2234 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_codes passes to ->, at line 2234 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2346	2346
Object	->	->

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2346.         memset(rar->lengthtable, 0, sizeof(rar->lengthtable));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=175
Status	New

The size of the buffer used by free_codes in ->, at line 2512 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that free_codes passes to ->, at line 2512 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2523	2523
Object	->	->

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	free_codes(struct archive_read *a)

```
....
2523.     memset(&rar->maincode, 0, sizeof(rar->maincode));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=176
Status	New

The size of the buffer used by free_codes in ->, at line 2512 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that free_codes passes to ->, at line 2512 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2524	2524
Object	->	->

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	free_codes(struct archive_read *a)

```
....
2524.     memset(&rar->offsetcode, 0, sizeof(rar->offsetcode));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=177
Status	New

The size of the buffer used by free_codes in ->, at line 2512 of ravynos-1/archive_read_support_format_rar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that free_codes passes to ->, at line 2512 of ravynos-1/archive_read_support_format_rar.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2525	2525
Object	->	->

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method free_codes(struct archive_read *a)

```
....
2525.     memset(&rar->lowoffsetcode, 0, sizeof(rar->lowoffsetcode));
```

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=1070095&projectid=70085&pathid=921
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7144	7144
Object	result	result

Code Snippet
File Name ravynos-1/authzone.c
Method dup_all(char* str)

```
....
7144.         char* result = strdup(str);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=922
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	72	72
Object	ipsecmod_env	ipsecmod_env

Code Snippet
File Name ravynos-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 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=923
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	1869	1869
Object	ds	ds

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lzh_decode_init(struct lzh_stream *strm, const char *method)

```
....
1869.            strm->ds = calloc(1, sizeof(*strm->ds));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=924
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	1896	1896
Object	w_buff	w_buff

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lzh_decode_init(struct lzh_stream *strm, const char *method)

```
....
1896.               ds->w_buff = malloc(ds->w_size);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=925
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	822	822
Object	value	value

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method add_option(struct archive_read *a, struct mtree_option **global,

```
....
822.         if ((opt->value = malloc(len + 1)) == NULL) {
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=926
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	929	929

Object	entry	entry

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method process_add_entry(struct archive_read *a, struct mtree *mtree,

```
....
929.        if ((entry = malloc(sizeof(*entry))) == NULL) {
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=927
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	982	982
Object	name	name

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method process_add_entry(struct archive_read *a, struct mtree *mtree,

```
....
982.        if ((entry->name = malloc(name_len + 1)) == NULL) {
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=928
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1890	1890
Object	buff	buff

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method read_data(struct archive_read *a, const void **buff, size_t *size,

```
....
1890.            mtree->buff = malloc(mtree->buffsize);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=929
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1688	1688
Object	dbo	dbo

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	read_header(struct archive_read *a, struct archive_entry *entry,

```
....
1688.    if ((rar->dbo = calloc(1, sizeof(*rar->dbo))) == NULL)
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=930
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2774	2774
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	make_table(struct archive_read *a, struct huffman_code *code)

```
....
2774.    code->table =
```

Memory Leak\Path 11:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=931
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3100	3100
Object	unp_buffer	unp_buffer

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method copy_from_lzss_window_to_unp(struct archive_read *a, const void **buffer,

```
....
3100.       if ((rar->unp_buffer = malloc(rar->unp_buffer_size)) == NULL)
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=932
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3317	3317
Object	filter	filter

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3317.     filter = calloc(1, sizeof(*filter));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=933
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3322	3322
Object	globaldata	globaldata

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	create_filter(struct rar_program_code *prog, const uint8_t *globaldata, uint32_t globaldatalen, uint32_t registers[8], size_t startpos, uint32_t length)

```
....
3322.     filter->globaldata = calloc(1, filter->globaldatalen);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=934
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3383	3383
Object	vm	vm

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	run_filters(struct archive_read *a)

```
....
3383.      filters->vm = calloc(1, sizeof(*filters->vm));
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=935
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3446	3446

Object	prog	prog

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method compile_program(const uint8_t *bytes, size_t length)

```
....
3446.     prog = calloc(1, sizeof(*prog));
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=936
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3454	3454
Object	staticdata	staticdata

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method compile_program(const uint8_t *bytes, size_t length)

```
....
3454.       prog->staticdata = malloc(prog->staticdatalen);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=937
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	566	566
Object	zonefile	zonefile

Code Snippet
File Name ravynos-1/authzone.c
Method auth_zone_set_zonefile(struct auth_zone* z, char* zonefile)

```
....
566.                  z->zonefile = strdup(zonefile);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=938
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	801	801
Object	d	d

Code Snippet
File Name ravynos-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 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=939
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	954	954
Object	d	d

Code Snippet
File Name ravynos-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 20:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=940
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1017	1017
Object	sigd	sigd

Code Snippet

File Name	ravynos-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 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=941
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5626	5626
Object	a	a

Code Snippet

File Name	ravynos-1/authzone.c
Method	xfr_master_add_addrs(struct auth_master* m, struct ub_packed_rrset_key* rrset,

```
....
5626.              a = (struct auth_addr*)calloc(1, sizeof(*a));
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=942
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7111	7111
Object	m	m

Code Snippet
File Name ravynos-1/authzone.c
Method auth_master_new(struct auth_master*** list)

```
....
7111.        m = (struct auth_master*)calloc(1, sizeof(*m));
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=943
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7258	7258
Object	host	host

Code Snippet
File Name ravynos-1/authzone.c
Method xfer_set_masters(struct auth_master** list, struct config_auth* c,

```
....
7258.               m->host = strdup(p->str);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=944
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7268	7268
Object	host	host

Code Snippet

File Name ravynos-1/authzone.c
Method xfer_set_masters(struct auth_master** list, struct config_auth* c,

```
....
7268.                m->host = strdup(p->str);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=945
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	239	239
Object	sc	sc

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

```
....
239.          if ((sc = calloc(1, sizeof(*sc))) == NULL)
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=946
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2482	2482
Object	pre	pre

Code Snippet
File Name ravynos-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2482.         if ((pre = calloc(SSH_CHANNEL_MAX_TYPE, sizeof(*pre))) ==
NULL ||
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=947
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2483	2483
Object	post	post

Code Snippet
File Name ravynos-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2483.           (post = calloc(SSH_CHANNEL_MAX_TYPE, sizeof(*post))) ==
NULL)
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=948
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	499	499
Object	data	data

Code Snippet
File Name ravynos-1/cxgbtool.c
Method dump_regs(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
499.        if ((regs.data = malloc(regs.len)) == NULL)
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=949
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	618	618
Object	data	data

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	meminfo(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
618.          if ((regs.data = malloc(regs.len)) == NULL)
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=950
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1004	1004
Object	buf	buf

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	load_fw(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1004.         op.buf = malloc(MAX_FW_IMAGE_SIZE + 1);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=951
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1038	1038
Object	buf	buf

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	load_boot(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1038.        op.buf = malloc(MAX_BOOT_IMAGE_SIZE + 1);
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=952
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1575	1575
Object	data	data

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	get_up_la(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1575.        la.data = malloc(la.bufsize);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=953
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1609	1609
Object	data	data

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	get_up_ioqs(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1609.        ioqs.data = malloc(IOQS_BUFSIZE);
```

Memory Leak\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=954
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	816	816
Object	realm	realm

Code Snippet

File Name	ravynos-1/http.c
Method	http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
816.                              cs->challenges[cs->count]->realm =
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=955
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	819	819
Object	qop	qop

Code Snippet

File Name	ravynos-1/http.c
Method	http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
819.                              cs->challenges[cs->count]->qop =
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=956
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c

Line	822	822
Object	nonce	nonce

Code Snippet
File Name ravynos-1/http.c
Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
822.                    cs->challenges[cs->count]->nonce =
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=957
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	825	825
Object	opaque	opaque

Code Snippet
File Name ravynos-1/http.c
Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
825.                    cs->challenges[cs->count]->opaque =
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=958
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	828	828
Object	algo	algo

Code Snippet
File Name ravynos-1/http.c
Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
828.                              cs->challenges[cs->count]->algo =
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=959
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	982	982
Object	str	str

Code Snippet
File Name ravynos-1/http.c
Method http_base64(const char *src)

```
....
982.          if ((str = malloc(((l + 2) / 3) * 4 + 1)) == NULL)
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=960
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1069	1069
Object	scheme	scheme

Code Snippet
File Name ravynos-1/http.c
Method http_authfromenv(const char *p, http_auth_params_t *parms)

```
....
1069.         if ((parms->scheme = strdup(v)) == NULL) {
```

Memory Leak\Path 41:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=961
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1079	1079
Object	realm	realm

Code Snippet
File Name ravynos-1/http.c
Method http_authfromenv(const char *p, http_auth_params_t *parms)

```
....
1079.          if ((parms->realm = strdup(v)) == NULL) {
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=962
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1089	1089
Object	user	user

Code Snippet
File Name ravynos-1/http.c
Method http_authfromenv(const char *p, http_auth_params_t *parms)

```
....
1089.          if ((parms->user = strdup(v)) == NULL) {
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=963
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1096	1096

Object	password	password

Code Snippet
File Name ravynos-1/http.c
Method http_authfromenv(const char *p, http_auth_params_t *parms)

```
....
1096.        if ((parms->password = strdup(v)) == NULL) {
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=964
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1262	1262
Object	algo	algo

Code Snippet
File Name ravynos-1/http.c
Method http_digest_auth(conn_t *conn, const char *hdr, http_auth_challenge_t *c,

```
....
1262.                c->algo = strdup("");
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=965
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1270	1270
Object	qop	qop

Code Snippet
File Name ravynos-1/http.c
Method http_digest_auth(conn_t *conn, const char *hdr, http_auth_challenge_t *c,

```
....
1270.               c->qop = strdup("");
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=966
Status	New

	Source	Destination
File	ravynos-1/imsg.c	ravynos-1/imsg.c
Line	147	147
Object	data	data

Code Snippet
File Name ravynos-1/imsg.c
Method imsg_get(struct imsgbuf *ibuf, struct imsg *imsg)

```
....
147.         else if ((imsg->data = malloc(datalen)) == NULL)
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=967
Status	New

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1608	1608
Object	sort_buf	sort_buf

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

```
....
1608.        if ((sort_buf = calloc(2 * (g_nrecs + 1),
```

Memory Leak\Path 48:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=968
Status	New

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	2429	2429
Object	ctrl_info	ctrl_info

Code Snippet

File Name ravynos-1/mrsas.c

Method mrsas_init_fw(struct mrsas_softc *sc)

```
....
2429.        sc->ctrl_info = malloc(sizeof(struct mrsas_ctrl_info),
M_MRSAS, M_NOWAIT);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=969
Status	New

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	2480	2480
Object	streamDetectByLD	streamDetectByLD

Code Snippet

File Name ravynos-1/mrsas.c

Method mrsas_init_fw(struct mrsas_softc *sc)

```
....
2480.              sc->streamDetectByLD =
malloc(sizeof(PTR_LD_STREAM_DETECT) *
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=970
Status	New

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c

Line	2834	2834
Object	req_desc	req_desc

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_alloc_mpt_cmds(struct mrsas_softc *sc)

```
....
2834.		sc->req_desc = malloc(sc->request_alloc_sz, M_MRSAS,
M_NOWAIT);
```

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=1070095&projectid=70085&pathid=1470
Status	New

The variable declared in b at ravynos-1/a_d2i_fp.c in line 37 is not initialized when it is used by b at ravynos-1/a_d2i_fp.c in line 37.

	Source	Destination
File	ravynos-1/a_d2i_fp.c	ravynos-1/a_d2i_fp.c
Line	39	48
Object	b	b

Code Snippet
File Name ravynos-1/a_d2i_fp.c
Method void *ASN1_d2i_bio(void *(*xnew) (void), d2i_of_void *d2i, BIO *in, void **x)

```
....
39.	    BUF_MEM *b = NULL;
....
48.	    p = (unsigned char *)b->data;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1471
Status	New

The variable declared in b at ravynos-1/a_d2i_fp.c in line 57 is not initialized when it is used by b at ravynos-1/a_d2i_fp.c in line 57.

	Source	Destination
File	ravynos-1/a_d2i_fp.c	ravynos-1/a_d2i_fp.c
Line	59	68
Object	b	b

Code Snippet
File Name ravynos-1/a_d2i_fp.c
Method void *ASN1_item_d2i_bio(const ASN1_ITEM *it, BIO *in, void *x)

```
....
59.       BUF_MEM *b = NULL;
....
68.       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=1070095&projectid=70085&pathid=1472
Status	New

The variable declared in delete_list at ravynos-1/authzone.c in line 2201 is not initialized when it is used by delete_list at ravynos-1/authzone.c in line 2201.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	2204	2214
Object	delete_list	delete_list

Code Snippet
File Name ravynos-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=1070095&projectid=70085&pathid=1473
Status	New

The variable declared in cp at ravynos-1/authzone.c in line 5443 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5474	5497
Object	cp	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5474.           xfr->task_transfer->cp = NULL;
....
5497.           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=1070095&projectid=70085&pathid=1474
Status	New

The variable declared in next at ravynos-1/authzone.c in line 3966 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3978	5497
Object	next	cp

Code Snippet
File Name ravynos-1/authzone.c
Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3978.           m->next = NULL;
```

File Name ravynos-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.           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=1070095&projectid=70085&pathid=1475
Status	New

The variable declared in list at ravynos-1/authzone.c in line 3966 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3968	5497
Object	list	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3968.        struct auth_master* list = NULL, *last = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.            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=1070095&projectid=70085&pathid=1476
Status	New

The variable declared in scan_specific at ravynos-1/authzone.c in line 4137 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4149	5497
Object	scan_specific	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	xfr_transfer_nextmaster(struct auth_xfer* xfr)

```
....
4149.               xfr->task_transfer->scan_specific = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.               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=1070095&projectid=70085&pathid=1477
Status	New

The variable declared in scan_specific at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4066	5497
Object	scan_specific	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4066.         xfr->task_transfer->scan_specific = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.               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=1070095&projectid=70085&pathid=1478
Status	New

The variable declared in scan_addr at ravynos-1/authzone.c in line 3990 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3993	5497
Object	scan_addr	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_transfer_start_lookups(struct auth_xfer* xfr)

```
....
3993.        xfr->task_transfer->scan_addr = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.              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=1070095&projectid=70085&pathid=1479
Status	New

The variable declared in scan_target at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4057	5497
Object	scan_target	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4057.                xfr->task_transfer->scan_target = NULL;
```

▼

File Name ravynos-1/authzone.c

Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.            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=1070095&projectid=70085&pathid=1480
Status	New

The variable declared in scan_addr at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4058	5497
Object	scan_addr	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4058.                 xfr->task_transfer->scan_addr = NULL;
```

▼

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.            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=1070095&projectid=70085&pathid=1481
Status	New

The variable declared in scan_addr at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c

Line	4067	5497
Object	scan_addr	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4067.       xfr->task_transfer->scan_addr = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.             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=1070095&projectid=70085&pathid=1482
Status	New

The variable declared in worker at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6321	5497
Object	worker	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6321.       xfr->task_probe->worker = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.             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=1070095&projectid=70085&pathid=1483
Status	New

The variable declared in cp at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6319	5497
Object	cp	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6319.        xfr->task_probe->cp = NULL;
```

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.              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=1070095&projectid=70085&pathid=1484
Status	New

The variable declared in env at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6322	5497
Object	env	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6322.        xfr->task_probe->env = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.                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=1070095&projectid=70085&pathid=1485
Status	New

The variable declared in timer at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6316	5497
Object	timer	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6316.        xfr->task_probe->timer = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.                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=1070095&projectid=70085&pathid=1486
Status	New

The variable declared in next at ravynos-1/authzone.c in line 6023 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6029	5497
Object	next	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfer_link_data(sldns_buffer* pkt, struct auth_xfer* xfr)

```
....
6029.       e->next = NULL;
```

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5497.             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=1070095&projectid=70085&pathid=1487
Status	New

The variable declared in cp at ravynos-1/authzone.c in line 5443 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5474	5529
Object	cp	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5474.             xfr->task_transfer->cp = NULL;
....
5529.       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=1070095&projectid=70085&pathid=1488
Status	New

The variable declared in auth_name at ravynos-1/authzone.c in line 5443 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5448	5529
Object	auth_name	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5448.        char *auth_name = NULL;
....
5529.        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=1070095&projectid=70085&pathid=1489
Status	New

The variable declared in next at ravynos-1/authzone.c in line 3966 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3978	5529
Object	next	cp

Code Snippet

File Name ravynos-1/authzone.c

Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3978.              m->next = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.       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=1070095&projectid=70085&pathid=1490
Status	New

The variable declared in list at ravynos-1/authzone.c in line 3966 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3968	5529
Object	list	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3968.       struct auth_master* list = NULL, *last = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.       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=1070095&projectid=70085&pathid=1491
Status	New

The variable declared in scan_specific at ravynos-1/authzone.c in line 4137 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4149	5529
Object	scan_specific	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_nextmaster(struct auth_xfer* xfr)

```
....
4149.           xfr->task_transfer->scan_specific = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.       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=1070095&projectid=70085&pathid=1492
Status	New

The variable declared in scan_addr at ravynos-1/authzone.c in line 3990 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3993	5529
Object	scan_addr	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_start_lookups(struct auth_xfer* xfr)

```
....
3993.       xfr->task_transfer->scan_addr = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.        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=1070095&projectid=70085&pathid=1493
Status	New

The variable declared in scan_target at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4057	5529
Object	scan_target	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4057.                    xfr->task_transfer->scan_target = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.        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=1070095&projectid=70085&pathid=1494
Status	New

The variable declared in scan_addr at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c

Line	4058	5529
Object	scan_addr	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4058.                   xfr->task_transfer->scan_addr = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.         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=1070095&projectid=70085&pathid=1495
Status	New

The variable declared in scan_specific at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4066	5529
Object	scan_specific	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4066.         xfr->task_transfer->scan_specific = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.         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=1070095&projectid=70085&pathid=1496
Status	New

The variable declared in scan_addr at ravynos-1/authzone.c in line 4051 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	4067	5529
Object	scan_addr	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	xfr_transfer_start_list(struct auth_xfer* xfr, struct auth_master* spec)

```
....
4067.        xfr->task_transfer->scan_addr = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.        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=1070095&projectid=70085&pathid=1497
Status	New

The variable declared in env at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6322	5529
Object	env	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	xfr_probe_disown(struct auth_xfer* xfr)

```
....
6322.        xfr->task_probe->env = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.        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=1070095&projectid=70085&pathid=1498
Status	New

The variable declared in timer at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6316	5529
Object	timer	cp

Code Snippet

File Name	ravynos-1/authzone.c
Method	xfr_probe_disown(struct auth_xfer* xfr)

```
....
6316.        xfr->task_probe->timer = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.        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=1070095&projectid=70085&pathid=1499
Status	New

The variable declared in cp at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6319	5529
Object	cp	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6319.       xfr->task_probe->cp = NULL;
```

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.       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=1070095&projectid=70085&pathid=1500
Status	New

The variable declared in worker at ravynos-1/authzone.c in line 6312 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6321	5529
Object	worker	cp

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6321.        xfr->task_probe->worker = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.        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=1070095&projectid=70085&pathid=1501
Status	New

The variable declared in next at ravynos-1/authzone.c in line 6023 is not initialized when it is used by cp at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6029	5529
Object	next	cp

Code Snippet

File Name ravynos-1/authzone.c

Method xfer_link_data(sldns_buffer* pkt, struct auth_xfer* xfr)

```
....
6029.        e->next = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5529.        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=1070095&projectid=70085&pathid=1502

Status	New

The variable declared in auth_name at ravynos-1/authzone.c in line 5443 is not initialized when it is used by auth_name at ravynos-1/authzone.c in line 5443.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5448	5532
Object	auth_name	auth_name

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_init_fetch(struct auth_xfer* xfr, struct module_env* env)

```
....
5448.        char *auth_name = NULL;
....
5532.              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=1070095&projectid=70085&pathid=1503
Status	New

The variable declared in ctype at ravynos-1/channels.c in line 3074 is not initialized when it is used by remote_name at ravynos-1/channels.c in line 450.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3079	498
Object	ctype	remote_name

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

```
....
3079.        char *ctype = NULL, *listen_host = NULL;
```

File Name ravynos-1/channels.c
Method channel_new(struct ssh *ssh, char *ctype, int type, int rfd, int wfd, int efd,

```
....
498.        c->remote_name = xstrdup(remote_name);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1504
Status	New

The variable declared in addr at ravynos-1/channels.c in line 3667 is not initialized when it is used by listening_addr at ravynos-1/channels.c in line 3721.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3670	3864
Object	addr	listening_addr

Code Snippet

File Name ravynos-1/channels.c

Method channel_fwd_bind_addr(struct ssh *ssh, const char *listen_addr, int *wildcardp,

```
....
3670.        const char *addr = NULL;
```

File Name ravynos-1/channels.c

Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3864.              c->listening_addr = addr == NULL ? NULL :
xstrdup(addr);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1505
Status	New

The variable declared in tkey at ravynos-1/cms_enc.c in line 23 is not initialized when it is used by key at ravynos-1/cms_enc.c in line 23.

	Source	Destination
File	ravynos-1/cms_enc.c	ravynos-1/cms_enc.c
Line	104	126
Object	tkey	key

Code Snippet

File Name	ravynos-1/cms_enc.c
Method	BIO *cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
104.            tkey = NULL;
....
126.                    ec->key = tkey;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1506
Status	New

The variable declared in tkey at ravynos-1/cms_enc.c in line 23 is not initialized when it is used by key at ravynos-1/cms_enc.c in line 23.

	Source	Destination
File	ravynos-1/cms_enc.c	ravynos-1/cms_enc.c
Line	30	126
Object	tkey	key

Code Snippet

File Name	ravynos-1/cms_enc.c
Method	BIO *cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
30.       unsigned char *tkey = NULL;
....
126.                    ec->key = tkey;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1507
Status	New

The variable declared in ret at ravynos-1/ec_asn1.c in line 585 is not initialized when it is used by ret at ravynos-1/ec_asn1.c in line 585.

	Source	Destination
File	ravynos-1/ec_asn1.c	ravynos-1/ec_asn1.c
Line	588	764
Object	ret	ret

Code Snippet

File Name	ravynos-1/ec_asn1.c
Method	EC_GROUP *EC_GROUP_new_from_ecparameters(const ECPARAMETERS *params)

```
....
588.        EC_GROUP *ret = NULL, *dup = NULL;
....
764.            OPENSSL_free(ret->seed);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1508
Status	New

The variable declared in strpool at ravynos-1/name.c in line 938 is not initialized when it is used by strpool at ravynos-1/name.c in line 938.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	940	951
Object	strpool	strpool

Code Snippet

File Name	ravynos-1/name.c
Method	hx509_general_name_unparse(GeneralName *name, char **str)

```
....
940.        struct rk_strpool *strpool = NULL;
....
951.          strpool = rk_strpoolprintf(strpool, "otherName: %s", oid);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1509
Status	New

The variable declared in strpool at ravynos-1/name.c in line 938 is not initialized when it is used by strpool at ravynos-1/name.c in line 938.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	940	956
Object	strpool	strpool

Code Snippet

File Name	ravynos-1/name.c
Method	hx509_general_name_unparse(GeneralName *name, char **str)

```
....
940.       struct rk_strpool *strpool = NULL;
....
956.         strpool = rk_strpoolprintf(strpool, "rfc822Name: %.*s\n",
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1510
Status	New

The variable declared in strpool at ravynos-1/name.c in line 938 is not initialized when it is used by strpool at ravynos-1/name.c in line 938.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	940	961
Object	strpool	strpool

Code Snippet

File Name	ravynos-1/name.c
Method	hx509_general_name_unparse(GeneralName *name, char **str)

```
....
940.       struct rk_strpool *strpool = NULL;
....
961.         strpool = rk_strpoolprintf(strpool, "dNSName: %.*s\n",
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1511
Status	New

The variable declared in strpool at ravynos-1/name.c in line 938 is not initialized when it is used by strpool at ravynos-1/name.c in line 938.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	940	974
Object	strpool	strpool

Code Snippet
File Name ravynos-1/name.c
Method hx509_general_name_unparse(GeneralName *name, char **str)

```
....
940.       struct rk_strpool *strpool = NULL;
....
974.         strpool = rk_strpoolprintf(strpool, "directoryName: %s", s);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1512
Status	New

The variable declared in strpool at ravynos-1/name.c in line 938 is not initialized when it is used by strpool at ravynos-1/name.c in line 938.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	940	979
Object	strpool	strpool

Code Snippet
File Name ravynos-1/name.c
Method hx509_general_name_unparse(GeneralName *name, char **str)

```
....
940.       struct rk_strpool *strpool = NULL;
....
979.         strpool = rk_strpoolprintf(strpool, "URI: %.*s",
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1513
Status	New

The variable declared in strpool at ravynos-1/name.c in line 938 is not initialized when it is used by strpool at ravynos-1/name.c in line 938.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	940	986
Object	strpool	strpool

Code Snippet
File Name ravynos-1/name.c
Method hx509_general_name_unparse(GeneralName *name, char **str)

```
....
940.       struct rk_strpool *strpool = NULL;
....
986.         strpool = rk_strpoolprintf(strpool, "IPAddress: ");
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1514
Status	New

The variable declared in strpool at ravynos-1/name.c in line 938 is not initialized when it is used by strpool at ravynos-1/name.c in line 938.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	940	1013
Object	strpool	strpool

Code Snippet
File Name ravynos-1/name.c
Method hx509_general_name_unparse(GeneralName *name, char **str)

```
....
940.       struct rk_strpool *strpool = NULL;
....
1013.        strpool = rk_strpoolprintf(strpool, "registeredID: %s",
oid);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1515
Status	New

The variable declared in strpool at ravynos-1/name.c in line 729 is not initialized when it is used by strpool at ravynos-1/name.c in line 729.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	758	792
Object	strpool	strpool

Code Snippet
File Name ravynos-1/name.c
Method hx509_name_expand(hx509_context context,

```
....
758.            struct rk_strpool *strpool = NULL;
....
792.              strpool = rk_strpoolprintf(strpool, "%s", value);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1516
Status	New

The variable declared in strpool at ravynos-1/name.c in line 729 is not initialized when it is used by strpool at ravynos-1/name.c in line 729.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	758	766
Object	strpool	strpool

Code Snippet
File Name ravynos-1/name.c
Method hx509_name_expand(hx509_context context,

```
....
758.            struct rk_strpool *strpool = NULL;
....
766.              strpool = rk_strpoolprintf(strpool, "%.*s",
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1517
Status	New

The variable declared in reqbuf at ravynos-1/phttpget.c in line 293 is not initialized when it is used by reqbuf at ravynos-1/phttpget.c in line 293.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	426	441
Object	reqbuf	reqbuf

Code Snippet	
File Name	ravynos-1/phttpget.c
Method	main(int argc, char *argv[])

```
....
426.                                    reqbuf = NULL;
....
441.                              len = send(sd, reqbuf + reqbufpos,
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1518
Status	New

The variable declared in reqbuf at ravynos-1/phttpget.c in line 293 is not initialized when it is used by reqbuf at ravynos-1/phttpget.c in line 293.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	448	441
Object	reqbuf	reqbuf

Code Snippet	
File Name	ravynos-1/phttpget.c
Method	main(int argc, char *argv[])

```
....
448.                        reqbuf = NULL;
....
441.                              len = send(sd, reqbuf + reqbufpos,
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1519
Status	New

The variable declared in reqbuf at ravynos-1/phttpget.c in line 293 is not initialized when it is used by reqbuf at ravynos-1/phttpget.c in line 293.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	305	441
Object	reqbuf	reqbuf

Code Snippet

File Name	ravynos-1/phttpget.c
Method	main(int argc, char *argv[])

```
....
305.         char * reqbuf = NULL;    /* Request buffer */
....
441.                             len = send(sd, reqbuf + reqbufpos,
```

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=1070095&projectid=70085&pathid=324
Status	New

Calling free() (line 1673) on a variable that was not dynamically allocated (line 1673) in file ravynos-1/archive_read_support_format_lha.c may result with a crash.

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	1683	1683
Object	lha	lha

Code Snippet

File Name	ravynos-1/archive_read_support_format_lha.c
Method	archive_read_format_lha_cleanup(struct archive_read *a)

```
....
1683.        free(lha);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=325
Status	New

Calling free() (line 297) on a variable that was not dynamically allocated (line 297) in file ravynos-1/archive_read_support_format_mtree.c may result with a crash.

	Source	Destination

File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	309	309
Object	p	p

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method cleanup(struct archive_read *a)

```
....
309.                free(p);
```

MemoryFree on StackVariable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=326
Status New

Calling free() (line 297) on a variable that was not dynamically allocated (line 297) in file ravynos-1/archive_read_support_format_mtree.c may result with a crash.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	318	318
Object	mtree	mtree

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method cleanup(struct archive_read *a)

```
....
318.        free(mtree);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=327
Status New

Calling free() (line 1339) on a variable that was not dynamically allocated (line 1339) in file ravynos-1/archive_read_support_format_rar.c may result with a crash.

	Source	Destination

File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	1352	1352
Object	rar	rar

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method archive_read_format_rar_cleanup(struct archive_read *a)

```
....
1352.     free(rar);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=328
Status	New

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

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

Code Snippet
File Name ravynos-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=1070095&projectid=70085&pathid=329
Status	New

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

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c

Line	1592	1592
Object	n	n

Code Snippet
File Name ravynos-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=1070095&projectid=70085&pathid=330
Status	New

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

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

Code Snippet
File Name ravynos-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=1070095&projectid=70085&pathid=331
Status	New

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

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

Code Snippet	
File Name	ravynos-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=1070095&projectid=70085&pathid=332
Status	New

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

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

Code Snippet	
File Name	ravynos-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=1070095&projectid=70085&pathid=333
Status	New

Calling free() (line 699) on a variable that was not dynamically allocated (line 699) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	736	736
Object	s	s

Code Snippet	
File Name	ravynos-1/channels.c

Method channel_free(struct ssh *ssh, Channel *c)

```
....
736.                free(s);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=334
Status	New

Calling free() (line 985) on a variable that was not dynamically allocated (line 985) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	1027	1027
Object	cp	cp

Code Snippet

File Name ravynos-1/channels.c

Method channel_open_message(struct ssh *ssh)

```
....
1027.                           free(cp);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=335
Status	New

Calling free() (line 985) on a variable that was not dynamically allocated (line 985) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	1030	1030
Object	cp	cp

Code Snippet

File Name ravynos-1/channels.c

Method channel_open_message(struct ssh *ssh)

```
....
1030.                     free(cp);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=336
Status	New

Calling free() (line 1774) on a variable that was not dynamically allocated (line 1774) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	1819	1819
Object	remote_ipaddr	remote_ipaddr

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

```
....
1819.          free(remote_ipaddr);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=337
Status	New

Calling free() (line 1823) on a variable that was not dynamically allocated (line 1823) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	1878	1878
Object	local_ipaddr	local_ipaddr

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

```
....
1878.       free(local_ipaddr);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=338
Status	New

Calling free() (line 2135) on a variable that was not dynamically allocated (line 2135) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2170	2170
Object	data	data

Code Snippet

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

```
....
2170.             free(data);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=339
Status	New

Calling free() (line 3074) on a variable that was not dynamically allocated (line 3074) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3214	3214
Object	ctype	ctype

Code Snippet

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

```
....
3214.        free(ctype);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=340
Status	New

Calling free() (line 3074) on a variable that was not dynamically allocated (line 3074) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3215	3215
Object	listen_host	listen_host

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

```
....
3215.        free(listen_host);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=341
Status	New

Calling free() (line 3548) on a variable that was not dynamically allocated (line 3548) in file ravynos-1/channels.c may result with a crash.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3573	3573
Object	msg	msg

Code Snippet
File Name ravynos-1/channels.c
Method channel_input_open_failure(int type, u_int32_t seq, struct ssh *ssh)

```
....
3573.        free(msg);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=342
Status	New

Calling free() (line 3377) on a variable that was not dynamically allocated (line 3377) in file ravynos-1/cxgbetool.c may result with a crash.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3435	3435
Object	line	line

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	parse_offload_policy(const char *fname, struct t4_offload_policy *op)

```
....
3435.        free(line);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=343
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	126	126
Object	inputline	inputline

Code Snippet

File Name	ravynos-1/gvinum.c
Method	main(int argc, char **argv)

```
....
126.                              free(inputline);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=344
Status	New

Calling free() (line 175) on a variable that was not dynamically allocated (line 175) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	352	352
Object	sdname	sdname

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
352.                                    free(sdname);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=345
Status	New

Calling free() (line 421) on a variable that was not dynamically allocated (line 421) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	469	469
Object	dname	dname

Code Snippet

File Name	ravynos-1/gvinum.c
Method	create_drive(const char *device)

```
....
469.                    free(dname);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=346
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1295	1295
Object	s	s

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1295.            free(s);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=347
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1302	1302
Object	s	s

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1302.               free(s);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=348
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1303	1303
Object	d	d

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1303.               free(d);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=349
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1316	1316
Object	s	s

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1316.            free(s);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=350
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1317	1317
Object	d	d

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1317.            free(d);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=351
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1318	1318
Object	drive	drive

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1318.                 free(drive);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=352
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1322	1322
Object	sdname	sdname

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1322.         free(sdname);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=353
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1338	1338
Object	drive	drive

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1338.        free(drive);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=354
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1341	1341
Object	s	s

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1341.            free(s);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=355
Status	New

Calling free() (line 1270) on a variable that was not dynamically allocated (line 1270) in file ravynos-1/gvinum.c may result with a crash.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1342	1342
Object	d	d

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_grow(int argc, char * const *argv)

```
....
1342.               free(d);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=356
Status	New

Calling free() (line 317) on a variable that was not dynamically allocated (line 317) in file ravynos-1/http.c may result with a crash.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	325	325
Object	io	io

Code Snippet
File Name ravynos-1/http.c
Method http_closefn(void *v)

```
....
325.         free(io);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=357
Status	New

Calling free() (line 392) on a variable that was not dynamically allocated (line 392) in file ravynos-1/http.c may result with a crash.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	410	410
Object	msg	msg

Code Snippet
File Name ravynos-1/http.c
Method http_cmd(conn_t *conn, const char *fmt, ...)

```
....
410.        free(msg);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=358
Status	New

Calling free() (line 1249) on a variable that was not dynamically allocated (line 1249) in file ravynos-1/http.c may result with a crash.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1303	1303
Object	options	options

Code Snippet
File Name ravynos-1/http.c
Method http_digest_auth(conn_t *conn, const char *hdr, http_auth_challenge_t *c,

```
....
1303.           free(options);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=359
Status	New

Calling free() (line 1525) on a variable that was not dynamically allocated (line 1525) in file ravynos-1/http.c may result with a crash.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1562	1562
Object	line	line

Code Snippet
File Name ravynos-1/http.c
Method http_print_html(FILE *out, FILE *in)

```
....
1562.         free(line);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=360
Status	New

Calling free() (line 1585) on a variable that was not dynamically allocated (line 1585) in file ravynos-1/http.c may result with a crash.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1899	1899
Object	neW	neW

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1899.                                     free(new);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=361
Status	New

Calling free() (line 272) on a variable that was not dynamically allocated (line 272) in file ravynos-1/imsg.c may result with a crash.

	Source	Destination
File	ravynos-1/imsg.c	ravynos-1/imsg.c
Line	282	282
Object	ifd	ifd

Code Snippet

File Name	ravynos-1/imsg.c
Method	imsg_get_fd(struct imsgbuf *ibuf)

```
....
282.         free(ifd);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=362
Status	New

Calling free() (line 88) on a variable that was not dynamically allocated (line 88) in file ravynos-1/ipsecmod.c may result with a crash.

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	96	96
Object	ipsecmod_env	ipsecmod_env

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_deinit(struct module_env* env, int id)

```
....
96.    free(ipsecmod_env);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=363
Status	New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file ravynos-1/ipsecmod.c may result with a crash.

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	283	283
Object	tempstring	tempstring

Code Snippet
File Name ravynos-1/ipsecmod.c
Method call_hook(struct module_qstate* qstate, struct ipsecmod_qstate* iq,

```
....
283.                free(tempstring);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=364
Status	New

Calling free() (line 249) on a variable that was not dynamically allocated (line 249) in file ravynos-1/ipsecmod.c may result with a crash.

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	287	287
Object	tempstring	tempstring

Code Snippet
File Name ravynos-1/ipsecmod.c
Method call_hook(struct module_qstate* qstate, struct ipsecmod_qstate* iq,

```
....
287.         free(tempstring);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=365
Status	New

Calling free() (line 1114) on a variable that was not dynamically allocated (line 1114) in file ravynos-1/lockstat.c may result with a crash.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1604	1604
Object	data_buf	data_buf

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

```
....
1604.               free(data_buf);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=366
Status	New

Calling free() (line 938) on a variable that was not dynamically allocated (line 938) in file ravynos-1/name.c may result with a crash.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	952	952
Object	oid	oid

Code Snippet
File Name ravynos-1/name.c
Method hx509_general_name_unparse(GeneralName *name, char **str)

```
....
952.         free(oid);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=367
Status	New

Calling free() (line 938) on a variable that was not dynamically allocated (line 938) in file ravynos-1/name.c may result with a crash.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	1014	1014
Object	oid	oid

Code Snippet
File Name ravynos-1/name.c
Method hx509_general_name_unparse(GeneralName *name, char **str)

```
....
1014.        free(oid);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=368
Status	New

Calling free() (line 293) on a variable that was not dynamically allocated (line 293) in file ravynos-1/phttpget.c may result with a crash.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	425	425
Object	reqbuf	reqbuf

Code Snippet

File Name	ravynos-1/phttpget.c
Method	main(int argc, char *argv[])

```
....
425.                                    free(reqbuf);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=369
Status	New

Calling free() (line 293) on a variable that was not dynamically allocated (line 293) in file ravynos-1/phttpget.c may result with a crash.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	447	447
Object	reqbuf	reqbuf

Code Snippet

File Name	ravynos-1/phttpget.c
Method	main(int argc, char *argv[])

```
....
447.                            free(reqbuf);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=370
Status	New

Calling free() (line 293) on a variable that was not dynamically allocated (line 293) in file ravynos-1/phttpget.c may result with a crash.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	718	718
Object	reqbuf	reqbuf

Code Snippet

File Name	ravynos-1/phttpget.c
Method	main(int argc, char *argv[])

```
....
718.                            free(reqbuf);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=371
Status	New

Calling free() (line 125) on a variable that was not dynamically allocated (line 125) in file ravynos-1/phttpget.c may result with a crash.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	179	179
Object	proxy_auth_userpass	proxy_auth_userpass

Code Snippet

File Name	ravynos-1/phttpget.c
Method	readenv(void)

```
....
179.            free(proxy_auth_userpass);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=372
Status	New

Calling free() (line 125) on a variable that was not dynamically allocated (line 125) in file ravynos-1/phttpget.c may result with a crash.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	180	180
Object	proxy_auth_userpass64	proxy_auth_userpass64

Code Snippet

File Name	ravynos-1/phttpget.c
Method	readenv(void)

```
....
180.            free(proxy_auth_userpass64);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=373
Status	New

Calling free() (line 307) on a variable that was not dynamically allocated (line 307) in file ravynos-1/scsi_ch.c may result with a crash.

	Source	Destination
File	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	315	315
Object	softc	softc

Code Snippet

File Name	ravynos-1/scsi_ch.c
Method	chcleanup(struct cam_periph *periph)

```
....
315.        free(softc, M_DEVBUF);
```

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=1070095&projectid=70085&pathid=392
Status	New

The function len in ravynos-1/cap_sendmsg.c at line 126 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	ravynos-1/cap_sendmsg.c	ravynos-1/cap_sendmsg.c
Line	153	153
Object	len	len

Code Snippet

File Name	ravynos-1/cap_sendmsg.c
Method	probe_defrouters(uint32_t ifindex, uint32_t linkid)

```
....
153.        buf = malloc(len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=393
Status	New

The function clip_buf_size in ravynos-1/cxgbetool.c at line 3488 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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3494	3494
Object	clip_buf_size	clip_buf_size

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	display_clip(void)

```
....
3494.        buf = malloc(clip_buf_size);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=394
Status	New

The function datalen in ravynos-1/imsg.c at line 126 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	ravynos-1/imsg.c	ravynos-1/imsg.c
Line	147	147
Object	datalen	datalen

Code Snippet

File Name	ravynos-1/imsg.c
Method	imsg_get(struct imsgbuf *ibuf, struct imsg *imsg)

```
....
147.        else if ((imsg->data = malloc(datalen)) == NULL)
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=395
Status	New

The function sz in ravynos-1/krb5_mech.c at line 158 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	163	163
Object	sz	sz

Code Snippet

File Name	ravynos-1/krb5_mech.c
Method	get_data(const uint8_t **pp, size_t *lenp, struct krb5_data *dp)

```
....
163.        dp->kd_data = malloc(sz, M_GSSAPI, M_WAITOK);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=396
Status	New

The function tolen in ravynos-1/name.c at line 83 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	ravynos-1/name.c	ravynos-1/name.c
Line	90	90
Object	tolen	tolen

Code Snippet

File Name	ravynos-1/name.c
Method	quote_string(const char *f, size_t len, int flags, size_t *rlen)

```
....
90.       to = malloc(tolen);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=397
Status	New

The function ctlen in ravynos-1/phttpget.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	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	91	91
Object	ctlen	ctlen

Code Snippet

File Name	ravynos-1/phttpget.c
Method	b64enc(const char *ptext)

```
....
91.    if ((ctext = malloc(ctlen)) == NULL)
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=398
Status	New

The function mlen in ravynos-1/pmcstudy.c at line 2095 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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2128	2128
Object	mlen	mlen

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	build_counters_from_header(FILE *io)

```
....
2128.        cnts = malloc(mlen);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=399
Status	New

The function sz in ravynos-1/pmcstudy.c at line 2334 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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2502	2502
Object	sz	sz

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	get_cpuid_set(void)

```
....
2502.              valid_pmcs = malloc(sz);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=400
Status	New

The function len in ravynos-1/pmcstudy.c at line 2334 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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2522	2522
Object	len	len

Code Snippet
File Name ravynos-1/pmcstudy.c
Method get_cpuid_set(void)

```
....
2522.              valid_pmcs[valid_pmc_cnt] = malloc(len);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=401
Status	New

The function sz in ravynos-1/pmcstudy.c at line 2334 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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2535	2535
Object	sz	sz

Code Snippet
File Name ravynos-1/pmcstudy.c
Method get_cpuid_set(void)

```
....
2535.                    more = malloc(sz);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=402
Status	New

The function len in ravynos-1/pmcstudy.c at line 2641 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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2658	2658
Object	len	len

Code Snippet
File Name ravynos-1/pmcstudy.c
Method add_it_to(char **vars, int cur_cnt, char *name)

```
....
2658.        vars[cur_cnt] = malloc(len);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=403
Status	New

The function mal in ravynos-1/pmcstudy.c at line 2669 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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2698	2698
Object	mal	mal

Code Snippet
File Name ravynos-1/pmcstudy.c
Method build_command_for_exp(struct expression *exp)

```
....
2698.        vars = malloc(mal);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=404
Status	New

The function size in ravynos-1/scsi_ch.c at line 1182 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	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	1306	1306
Object	size	size

Code Snippet
File Name ravynos-1/scsi_ch.c
Method chgetelemstatus(struct cam_periph *periph, int scsi_version, u_long cmd,

```
....
1306.        data = (caddr_t)malloc(size, M_DEVBUF, M_WAITOK);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=405
Status	New

The function len in ravynos-1/sctp_sys_calls.c at line 678 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	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	736	736
Object	len	len

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_sendx(int sd, const void *msg, size_t msg_len,

```
....
736.        buf = malloc(len);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=406
Status	New

The function len in ravynos-1/test_x509.c at line 49 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	56	56
Object	len	len

Code Snippet
File Name ravynos-1/test_x509.c
Method xmalloc(size_t len)

```
....
56.   buf = malloc(len);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=407
Status	New

The function slen in ravynos-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	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	218	218
Object	slen	slen

Code Snippet
File Name ravynos-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 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=408
Status	New

The function peer_count in ravynos-1/show.c at line 47 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	ravynos-1/show.c	ravynos-1/show.c
Line	56	56
Object	peer_count	peer_count

Code Snippet
File Name ravynos-1/show.c
Method static void sort_peers(struct wgdevice *device)

```
....
56.    peers = calloc(peer_count, sizeof(*peers));
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=409
Status	New

The function n in ravynos-1/test_x509.c at line 74 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	83	83
Object	n	n

Code Snippet
File Name ravynos-1/test_x509.c
Method xstrdup(const char *name)

```
....
83.    s = xmalloc(n);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=410
Status	New

The function nlen in ravynos-1/test_x509.c at line 106 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	118	118
Object	nlen	nlen

Code Snippet
File Name   ravynos-1/test_x509.c
Method   SB_expand(string_builder *sb, size_t extra_len)

```
....
118.         nbuf = xmalloc(nlen);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=411
Status	New

The function blen in ravynos-1/test_x509.c at line 403 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	409	409
Object	blen	blen

Code Snippet
File Name   ravynos-1/test_x509.c
Method   read_all(FILE *f, size_t *len)

```
....
409.        buf = xmalloc(blen);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=412
Status	New

The function blen in ravynos-1/test_x509.c at line 403 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	418	418
Object	blen	blen

Code Snippet

File Name	ravynos-1/test_x509.c
Method	read_all(FILE *f, size_t *len)

```
....
418.                buf2 = xmalloc(blen);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=413
Status	New

The function ptr in ravynos-1/test_x509.c at line 403 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	427	427
Object	ptr	ptr

Code Snippet

File Name	ravynos-1/test_x509.c
Method	read_all(FILE *f, size_t *len)

```
....
427.                    buf3 = xmalloc(ptr);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=414
Status	New

The function ptr in ravynos-1/test_x509.c at line 975 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1022	1022
Object	ptr	ptr

Code Snippet
File Name ravynos-1/test_x509.c
Method parse_hex(const char *name, long linenum, const char *value, size_t *len)

```
....
1022.                   buf = xmalloc(ptr);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=415
Status	New

The function len in ravynos-1/archive_read_support_format_mtree.c at line 813 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	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	822	822
Object	len	len

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method add_option(struct archive_read *a, struct mtree_option **global,

```
....
822.        if ((opt->value = malloc(len + 1)) == NULL) {
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=416
Status	New

The function name_len in ravynos-1/archive_read_support_format_mtree.c at line 919 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	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	982	982
Object	name_len	name_len

Code Snippet

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	process_add_entry(struct archive_read *a, struct mtree *mtree,

```
....
982.        if ((entry->name = malloc(name_len + 1)) == NULL) {
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=417
Status	New

The function num in ravynos-1/authzone.c at line 7125 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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7130	7130
Object	num	num

Code Snippet

File Name	ravynos-1/authzone.c
Method	dup_prefix(char* str, size_t num)

```
....
7130.       result = (char*)malloc(num+1);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=418
Status	New

The function k in ravynos-1/name.c at line 201 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	ravynos-1/name.c	ravynos-1/name.c
Line	244	244
Object	k	k

Code Snippet
File Name ravynos-1/name.c
Method _hx509_Name_to_string(const Name *n, char **str)

```
....
244.            ss = malloc(k + 1);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=419
Status	New

The function k in ravynos-1/name.c at line 201 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	ravynos-1/name.c	ravynos-1/name.c
Line	269	269
Object	k	k

Code Snippet
File Name ravynos-1/name.c
Method _hx509_Name_to_string(const Name *n, char **str)

```
....
269.                ss = malloc(k + 1);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=420
Status	New

The function len in ravynos-1/name.c at line 332 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	ravynos-1/name.c	ravynos-1/name.c
Line	345	345
Object	len	len

Code Snippet
File Name ravynos-1/name.c
Method dsstringprep(const DirectoryString *ds, uint32_t **rname, size_t *rlen)

```
....
345.          COPYVOIDARRAY(ds, ia5String, len, name);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=421
Status	New

The function len in ravynos-1/name.c at line 332 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	ravynos-1/name.c	ravynos-1/name.c
Line	350	350
Object	len	len

Code Snippet
File Name ravynos-1/name.c
Method dsstringprep(const DirectoryString *ds, uint32_t **rname, size_t *rlen)

```
....
350.        COPYVOIDARRAY(ds, printableString, len, name);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=422
Status	New

The function len in ravynos-1/name.c at line 332 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	ravynos-1/name.c	ravynos-1/name.c
Line	354	354
Object	len	len

Code Snippet

File Name ravynos-1/name.c

Method dsstringprep(const DirectoryString *ds, uint32_t **rname, size_t *rlen)

```
....
354.        COPYCHARARRAY(ds, teletexString, len, name);
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=423
Status	New

The function len in ravynos-1/name.c at line 332 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	ravynos-1/name.c	ravynos-1/name.c
Line	358	358
Object	len	len

Code Snippet

File Name ravynos-1/name.c

Method dsstringprep(const DirectoryString *ds, uint32_t **rname, size_t *rlen)

```
....
358.        COPYVALARRAY(ds, bmpString, len, name);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=424
Status	New

The function len in ravynos-1/name.c at line 332 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	ravynos-1/name.c	ravynos-1/name.c
Line	362	362
Object	len	len

Code Snippet

File Name	ravynos-1/name.c
Method	dsstringprep(const DirectoryString *ds, uint32_t **rname, size_t *rlen)

```
....
362.        COPYVALARRAY(ds, universalString, len, name);
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=425
Status	New

The function len in ravynos-1/name.c at line 332 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	ravynos-1/name.c	ravynos-1/name.c
Line	369	369
Object	len	len

Code Snippet

File Name	ravynos-1/name.c
Method	dsstringprep(const DirectoryString *ds, uint32_t **rname, size_t *rlen)

```
....
369.        name = malloc(len * sizeof(name[0]));
```

Wrong Size t Allocation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=426
Status	New

The function pstr_len in ravynos-1/name.c at line 572 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	ravynos-1/name.c	ravynos-1/name.c
Line	636	636
Object	pstr_len	pstr_len

Code Snippet

File Name	ravynos-1/name.c
Method	hx509_parse_name(hx509_context context, const char *str, hx509_name *name)

```
....
636.            r = malloc(pstr_len + 1);
```

Wrong Size t Allocation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=427
Status	New

The function mal in ravynos-1/pmcstudy.c at line 2669 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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2718	2718
Object	mal	mal

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	build_command_for_exp(struct expression *exp)

```
....
2718.        cmd = malloc((mal+2));
```

Wrong Size t Allocation\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=428
Status	New

The function rdatalen in ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	803	803
Object	rdatalen	rdatalen

Code Snippet
File Name ravynos-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 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=429
Status	New

The function sigsz in ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	956	956
Object	sigsz	sigsz

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

```
....
956.                + sigsz);
```

Wrong Size t Allocation\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=430
Status	New

The function sigsz in ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1019	1019
Object	sigsz	sigsz

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

```
....
1019.               - sigsz);
```

Wrong Size t Allocation\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=431
Status	New

The function len in ravynos-1/test_x509.c at line 2021 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	2049	2049
Object	len	len

Code Snippet
File Name	ravynos-1/test_x509.c
Method	main(int argc, const char *argv[])

```
....
2049.                    dn = xmalloc(len + 1);
```

Wrong Size t Allocation\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=432
Status	New

The function n2 in ravynos-1/test_x509.c at line 265 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	272	272
Object	n2	n2

Code Snippet

File Name	ravynos-1/test_x509.c
Method	HT_expand(HT *ht)

```
....
272.        new_buckets = xmalloc(n2 * sizeof *new_buckets);
```

Wrong Size t Allocation\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=433
Status	New

The function len in ravynos-1/test_x509.c at line 790 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	817	817
Object	len	len

Code Snippet

File Name	ravynos-1/test_x509.c
Method	parse_header_name(void)

```
....
817.        name = xmalloc(len + 1);
```

Wrong Size t Allocation\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=434
Status	New

The function u in ravynos-1/test_x509.c at line 829 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	844	844
Object	u	u

Code Snippet
File Name ravynos-1/test_x509.c
Method parse_keyvalue(HT *d)

```
....
844.        name = xmalloc(u + 1);
```

Wrong Size t Allocation\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=435
Status	New

The function all_chains_len in ravynos-1/test_x509.c at line 1146 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1300	1300
Object	all_chains_len	all_chains_len

Code Snippet
File Name ravynos-1/test_x509.c
Method parse_object(char *objtype, HT *objdata, long linenum)

```
....
1300.                                   all_chains_len * sizeof
*all_chains);
```

Wrong Size t Allocation\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=436
Status	New

The function nlen in ravynos-1/test_x509.c at line 1146 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1306	1306
Object	nlen	nlen

Code Snippet
File Name ravynos-1/test_x509.c
Method parse_object(char *objtype, HT *objdata, long linenum)

```
....
1306.                               ntc = xmalloc(nlen * sizeof *ntc);
```

Wrong Size t Allocation\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=437
Status	New

The function num_anchors in ravynos-1/test_x509.c at line 1457 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1492	1492
Object	num_anchors	num_anchors

Code Snippet
File Name ravynos-1/test_x509.c
Method run_test_case(test_case *tc)

```
....
1492.        anchors = xmalloc(num_anchors * sizeof *anchors);
```

Wrong Size t Allocation\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=438
Status	New

The function num_certs in ravynos-1/test_x509.c at line 1457 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1519	1519
Object	num_certs	num_certs

Code Snippet

File Name	ravynos-1/test_x509.c
Method	run_test_case(test_case *tc)

```
....
1519.        certs = xmalloc(num_certs * sizeof *certs);
```

Wrong Size t Allocation\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=439
Status	New

The function num_names in ravynos-1/test_x509.c at line 1836 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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1865	1865
Object	num_names	num_names

Code Snippet

File Name	ravynos-1/test_x509.c
Method	test_name_extraction(void)

```
....
1865.        names = xmalloc(num_names * sizeof *names);
```

Wrong Size t Allocation\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=440
Status	New

The function len in ravynos-1/servconf.c at line 1345 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	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2335	2335
Object	len	len

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2335.                options->adm_forced_command = xstrdup(str +
len);
```

Wrong Size t Allocation\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=441
Status	New

The function len in ravynos-1/servconf.c at line 1345 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	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2410	2410
Object	len	len

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2410.                      options->version_addendum = xstrdup(str +
len);
```

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=1070095&projectid=70085&pathid=853
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2430	2382
Object	tree	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2430.              free(precode.tree);
....
2382.          free(precode.tree);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=854
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2438	2382
Object	tree	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2438.                 free(precode.tree);
....
2382.             free(precode.tree);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=855
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2404	2382
Object	tree	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2404.                 free(precode.tree);
....
2382.             free(precode.tree);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=856
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2412	2382
Object	tree	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c

Method	parse_codes(struct archive_read *a)

```
....
2412.                free(precode.tree);
....
2382.            free(precode.tree);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=857
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2413	2382
Object	table	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2413.                free(precode.table);
....
2382.            free(precode.tree);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=858
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2405	2382
Object	table	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2405.                 free(precode.table);
....
2382.             free(precode.tree);
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=859
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2431	2382
Object	table	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2431.                 free(precode.table);
....
2382.             free(precode.tree);
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=860
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2439	2382
Object	table	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2439.                   free(precode.table);
....
2382.               free(precode.tree);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=861
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2413	2383
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2413.                   free(precode.table);
....
2383.               free(precode.table);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=862
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2405	2383
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2405.               free(precode.table);
....
2383.           free(precode.table);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=863
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2439	2383
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2439.               free(precode.table);
....
2383.           free(precode.table);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=864
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2431	2383
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2431.                free(precode.table);
....
2383.            free(precode.table);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=865
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2430	2383
Object	tree	table

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2430.                free(precode.tree);
....
2383.            free(precode.table);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=866
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2438	2383
Object	tree	table

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2438.                 free(precode.tree);
....
2383.             free(precode.table);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=867
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2404	2383
Object	tree	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2404.                 free(precode.tree);
....
2383.             free(precode.table);
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=868
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2412	2383
Object	tree	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2412.               free(precode.tree);
....
2383.           free(precode.table);
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=869
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2412	2395
Object	tree	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2412.               free(precode.tree);
....
2395.             free(precode.tree);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=870
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2438	2395
Object	tree	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2438.                   free(precode.tree);
....
2395.                 free(precode.tree);
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=871
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2404	2395
Object	tree	tree

Code Snippet	
File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2404.                   free(precode.tree);
....
2395.                 free(precode.tree);
```

Double Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=872
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2430	2395
Object	tree	tree

Code Snippet	
File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2430.                  free(precode.tree);
....
2395.                free(precode.tree);
```

Double Free\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=873
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2431	2395
Object	table	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2431.                  free(precode.table);
....
2395.                free(precode.tree);
```

Double Free\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=874
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2439	2395
Object	table	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2439.               free(precode.table);
....
2395.             free(precode.tree);
```

Double Free\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=875
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2405	2395
Object	table	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2405.               free(precode.table);
....
2395.             free(precode.tree);
```

Double Free\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=876
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2413	2395
Object	table	tree

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2413.                free(precode.table);
....
2395.              free(precode.tree);
```

Double Free\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=877
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2431	2396
Object	table	table

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2431.                free(precode.table);
....
2396.              free(precode.table);
```

Double Free\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=878
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2439	2396
Object	table	table

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2439.                   free(precode.table);
....
2396.                 free(precode.table);
```

Double Free\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=879
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2413	2396
Object	table	table

Code Snippet	
File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2413.                   free(precode.table);
....
2396.                 free(precode.table);
```

Double Free\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=880
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2405	2396
Object	table	table

Code Snippet	
File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2405.                   free(precode.table);
....
2396.                 free(precode.table);
```

Double Free\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=881
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2430	2396
Object	tree	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2430.                   free(precode.tree);
....
2396.                 free(precode.table);
```

Double Free\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=882
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2438	2396
Object	tree	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2438.                   free(precode.tree);
....
2396.                 free(precode.table);
```

Double Free\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=883
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2404	2396
Object	tree	table

Code Snippet

File Name ravynos-1/archive_read_support_format_rar.c

Method parse_codes(struct archive_read *a)

```
....
2404.                   free(precode.tree);
....
2396.                 free(precode.table);
```

Double Free\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=884
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2412	2396
Object	tree	table

Code Snippet

File Name ravynos-1/archive_read_support_format_rar.c

Method parse_codes(struct archive_read *a)

```
....
2412.                 free(precode.tree);
....
2396.               free(precode.table);
```

Double Free\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=885
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2438	2450
Object	tree	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2438.                 free(precode.tree);
....
2450.       free(precode.tree);
```

Double Free\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=886
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2404	2450
Object	tree	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2404.                  free(precode.tree);
....
2450.          free(precode.tree);
```

Double Free\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=887
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2412	2450
Object	tree	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2412.                  free(precode.tree);
....
2450.          free(precode.tree);
```

Double Free\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=888
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2430	2450
Object	tree	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2430.               free(precode.tree);
....
2450.       free(precode.tree);
```

Double Free\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=889
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2405	2450
Object	table	tree

Code Snippet	
File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2405.               free(precode.table);
....
2450.       free(precode.tree);
```

Double Free\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=890
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2431	2450
Object	table	tree

Code Snippet	
File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2431.                   free(precode.table);
....
2450.           free(precode.tree);
```

Double Free\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=891
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2439	2450
Object	table	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2439.                   free(precode.table);
....
2450.           free(precode.tree);
```

Double Free\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=892
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2413	2450
Object	table	tree

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method parse_codes(struct archive_read *a)

```
....
2413.                 free(precode.table);
....
2450.         free(precode.tree);
```

Double Free\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=893
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2413	2451
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2413.                 free(precode.table);
....
2451.         free(precode.table);
```

Double Free\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=894
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2405	2451
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2405.                 free(precode.table);
....
2451.         free(precode.table);
```

Double Free\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=895
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2439	2451
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2439.                 free(precode.table);
....
2451.         free(precode.table);
```

Double Free\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=896
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2431	2451
Object	table	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2431.                   free(precode.table);
....
2451.         free(precode.table);
```

Double Free\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=897
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2412	2451
Object	tree	table

Code Snippet

File Name ravynos-1/archive_read_support_format_rar.c

Method parse_codes(struct archive_read *a)

```
....
2412.                   free(precode.tree);
....
2451.         free(precode.table);
```

Double Free\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=898
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2404	2451
Object	tree	table

Code Snippet

File Name ravynos-1/archive_read_support_format_rar.c

Method parse_codes(struct archive_read *a)

```
....
2404.                   free(precode.tree);
....
2451.          free(precode.table);
```

Double Free\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=899
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2438	2451
Object	tree	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2438.                   free(precode.tree);
....
2451.          free(precode.table);
```

Double Free\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=900
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	2430	2451
Object	tree	table

Code Snippet

File Name	ravynos-1/archive_read_support_format_rar.c
Method	parse_codes(struct archive_read *a)

```
....
2430.              free(precode.tree);
....
2451.      free(precode.table);
```

Double Free\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=901
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	1027	1030
Object	cp	cp

Code Snippet

File Name	ravynos-1/channels.c
Method	channel_open_message(struct ssh *ssh)

```
....
1027.                         free(cp);
....
1030.                   free(cp);
```

Double Free\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=902
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1048	1321
Object	password	upw

Code Snippet

File Name	ravynos-1/http.c
Method	clean_http_auth_params(http_auth_params_t *s)

```
....
1048.             free(s->password);
```

File Name	ravynos-1/http.c
Method	http_basic_auth(conn_t *conn, const char *hdr, const char *usr, const char *pwd)

```
....
1321.        free(upw);
```

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=1070095&projectid=70085&pathid=467
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 703 of ravynos-1/bsd-snprintf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/bsd-snprintf.c	ravynos-1/bsd-snprintf.c
Line	773	773
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/bsd-snprintf.c
Method	fmtfp (char *buffer, size_t *currlen, size_t maxlen,

```
....
773.              idx = (int) ((temp -intpart +0.05)* 10.0);
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=468
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 703 of ravynos-1/bsd-snprintf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	ravynos-1/bsd-snprintf.c	ravynos-1/bsd-snprintf.c
Line	788	788
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/bsd-snprintf.c
Method fmtfp (char *buffer, size_t *currlen, size_t maxlen,

```
....
788.                    idx = (int) ((temp -fracpart +0.05)* 10.0);
```

Integer Overflow\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=469
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1000 of ravynos-1/archive_read_support_format_lha.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	1033	1033
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method lha_read_file_header_2(struct archive_read *a, struct lha *lha)

```
....
1033.         padding = (int)lha->header_size - (int)(H2_FIXED_SIZE +
extdsize);
```

Integer Overflow\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=470
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 379 of ravynos-1/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c

Line	393	393
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/b_print.c
Method fmtstr(char **sbuffer,

```
....
393.        padlen = min - strln;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=471
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 561 of ravynos-1/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c
Line	635	635
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/b_print.c
Method fmtfp(char **sbuffer,

```
....
635.                    max -= (exp + 1);
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=472
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 561 of ravynos-1/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c
Line	715	715
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ravynos-1/b_print.c
Method	fmtfp(char **sbuffer,

```
....
715.                tmpexp = -exp;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=473
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 561 of ravynos-1/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c
Line	717	717
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ravynos-1/b_print.c
Method	fmtfp(char **sbuffer,

```
....
717.                tmpexp = exp;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=474
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1381 of ravynos-1/cxgbetool.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	1450	1450
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ravynos-1/cxgbetool.c
Method	filter_cmd(int argc, const char *argv[], int hashfilter)

```
....
1450.                   prio = (int)val;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=475
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2258 of ravynos-1/cxgbetool.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2277	2277
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/cxgbetool.c
Method read_tcb(int argc, const char *argv[])

```
....
2277.         tid = 1;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=476
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 57 of ravynos-1/e_chacha20_poly1305.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/e_chacha20_poly1305.c	ravynos-1/e_chacha20_poly1305.c
Line	81	81
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/e_chacha20_poly1305.c
Method static int chacha_cipher(EVP_CIPHER_CTX * ctx, unsigned char *out,

```
....
81.         rem = (unsigned int)(len % CHACHA_BLK_SIZE);
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=477
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 57 of ravynos-1/e_chacha20_poly1305.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/e_chacha20_poly1305.c	ravynos-1/e_chacha20_poly1305.c
Line	100	100
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/e_chacha20_poly1305.c
Method	static int chacha_cipher(EVP_CIPHER_CTX * ctx, unsigned char *out,

```
....
100.            ctr32 += (unsigned int)blocks;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=478
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1399 of ravynos-1/krb5_mech.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1431	1431
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/krb5_mech.c
Method	krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1431.                       EC = mlen % mblen;
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=479
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1399 of ravynos-1/krb5_mech.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1468	1468
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1468.               EC = cklen;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=480
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1953 of ravynos-1/lockstat.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1960	1960
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/lockstat.c
Method report_trace(FILE *out, lsrec_t **sort_buf)

```
....
1960.          rectype = g_recsize;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=481
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1753 of ravynos-1/lockstat.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1767	1767
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/lockstat.c
Method report_stats(FILE *out, lsrec_t **sort_buf, size_t nrecs, uint64_t total_count,

```
....
1767.        rectype = g_recsize;
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=482
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2334 of ravynos-1/pmcstudy.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2362	2362
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/pmcstudy.c
Method get_cpuid_set(void)

```
....
2362.        model = (((eax & 0xF0000) >> 12) | ((eax & 0xF0) >> 4));
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=483
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 128 of ravynos-1/xgbe-dev.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	ravynos-1/xgbe-dev.c	ravynos-1/xgbe-dev.c
Line	141	141
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/xgbe-dev.c
Method	xgbe_usec_to_riwt(struct xgbe_prv_data *pdata, unsigned int usec)

```
....
141.        ret = (usec * (rate / 1000000)) / 256;
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=484
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 147 of ravynos-1/xgbe-dev.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/xgbe-dev.c	ravynos-1/xgbe-dev.c
Line	160	160
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/xgbe-dev.c
Method	xgbe_riwt_to_usec(struct xgbe_prv_data *pdata, unsigned int riwt)

```
....
160.        ret = (riwt * 256) / (rate / 1000000);
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=485
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 87 of ravynos-1/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c
Line	106	106
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/b_print.c
Method _dopr(char **sbuffer,

```
....
106.        flags = currlen = cflags = min = 0;
```

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=1070095&projectid=70085&pathid=1005
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1039.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1048	1154
Object	password	MD5_Update

Code Snippet
File Name ravynos-1/http.c
Method clean_http_auth_params(http_auth_params_t *s)

```
....
1048.             free(s->password);
```

File Name ravynos-1/http.c
Method DigestCalcHA1(

```
....
1154.         MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 2:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1006
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1379.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1422	1154
Object	password	MD5_Update

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1422.                                aparams.password = strdup(purl->pwd);
```

File Name	ravynos-1/http.c
Method	DigestCalcHA1(

```
....
1154.        MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1007
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1379.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1432	1154
Object	password	MD5_Update

Code Snippet

File Name	ravynos-1/http.c
Method	http_connect(struct url *URL, struct url *purl, const char *flags)

```
....
1432.                                aparams.password = strdup(purl->pwd);
```

▼

File Name	ravynos-1/http.c
Method	DigestCalcHA1(

```
....
1154.         MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1008
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information pwd, from ravynos-1/http.c at line 1311.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1318	1154
Object	pwd	MD5_Update

Code Snippet

File Name	ravynos-1/http.c
Method	http_basic_auth(conn_t *conn, const char *hdr, const char *usr, const char *pwd)

```
....
1318.         if (asprintf(&upw, "%s:%s", usr, pwd) == -1)
```

▼

File Name	ravynos-1/http.c
Method	DigestCalcHA1(

```
....
1154.         MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1009
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information pszPassword, from ravynos-1/http.c at line 1140.

	Source	Destination

File	ravynos-1/http.c	ravynos-1/http.c
Line	1158	1158
Object	pszPassword	MD5_Update

Code Snippet

File Name	ravynos-1/http.c
Method	DigestCalcHA1(

```
....
1158.        MD5Update(&Md5Ctx, pszPassword, strlen(pszPassword));
```

Inadequate Encryption Strength\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1010
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information pszPassword, from ravynos-1/http.c at line 1140.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1158	1154
Object	pszPassword	MD5_Update

Code Snippet

File Name	ravynos-1/http.c
Method	DigestCalcHA1(

```
....
1158.        MD5Update(&Md5Ctx, pszPassword, strlen(pszPassword));
....
1154.        MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1011
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1585.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1723	1154

Object	password	MD5_Update

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1723.                           aparams.password = strdup(url->pwd);
```

File Name ravynos-1/http.c

Method DigestCalcHA1(

```
....
1154.        MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1012
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1175 of ravynos-1/http.c, to protect sensitive personal information pwd, from ravynos-1/http.c at line 1585.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1906	1200
Object	pwd	MD5_Update

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1906.                                     url->port, p, url->user, url-
>pwd);
```

File Name ravynos-1/http.c

Method DigestCalcResponse(

```
....
1200.        MD5Update(&Md5Ctx, pszDigestUri, strlen(pszDigestUri));
```

Inadequate Encryption Strength\Path 9:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1013
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1585.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1732	1154
Object	password	MD5_Update

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1732.                         aparams.password = strdup(url->pwd);
```

File Name ravynos-1/http.c
Method DigestCalcHA1(

```
....
1154.         MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1014
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1585.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1736	1154
Object	password	MD5_Update

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1736.                           aparams.password = strdup(url->pwd);
```

▼

File Name	ravynos-1/http.c
Method	DigestCalcHA1(

```
....
1154.           MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1015
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1585.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1693	1154
Object	password	MD5_Update

Code Snippet

File Name	ravynos-1/http.c
Method	http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1693.                           aparams.password = strdup(purl->pwd);
```

▼

File Name	ravynos-1/http.c
Method	DigestCalcHA1(

```
....
1154.           MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1016
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information password, from ravynos-1/http.c at line 1585.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1702	1154
Object	password	MD5_Update

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1702.                         aparams.password = strdup(purl->pwd);
```

File Name ravynos-1/http.c
Method DigestCalcHA1(

```
....
1154.        MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName));
```

Inadequate Encryption Strength\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1017
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1140 of ravynos-1/http.c, to protect sensitive personal information pszPassword, from ravynos-1/http.c at line 1140.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1158	1158
Object	pszPassword	MD5_Update

Code Snippet
File Name ravynos-1/http.c
Method DigestCalcHA1(

```
....
1158.        MD5Update(&Md5Ctx, pszPassword, strlen(pszPassword));
```

Inadequate Encryption Strength\Path 14:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1018
Status	New

The application uses a weak cryptographic algorithm, MD5_Update at line 1175 of ravynos-1/http.c, to protect sensitive personal information pwd, from ravynos-1/http.c at line 1585.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1919	1200
Object	pwd	MD5_Update

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1919.                                   strcpy(new->pwd, url->pwd);
```

File Name ravynos-1/http.c

Method DigestCalcResponse(

```
....
1200.        MD5Update(&Md5Ctx, pszDigestUri, strlen(pszDigestUri));
```

Inadequate Encryption Strength\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1019
Status	New

The application uses a weak cryptographic algorithm, DES_crypt at line 98 of ravynos-1/xcrypt.c, to protect sensitive personal information password, from ravynos-1/xcrypt.c at line 98.

	Source	Destination
File	ravynos-1/xcrypt.c	ravynos-1/xcrypt.c
Line	113	113
Object	password	DES_crypt

Code Snippet

File Name ravynos-1/xcrypt.c

Method xcrypt(const char *password, const char *salt)

```
....
113.                crypted = crypt(password, salt);
```

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=1070095&projectid=70085&pathid=454
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1531 of ravynos-1/archive_read_support_format_mtree.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1586	1586
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method parse_digest(struct archive_read *a, struct archive_entry *entry,

```
....
1586.             digest_buf[j] = high << 4 | low;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=455
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 273 of ravynos-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	ravynos-1/buf.c	ravynos-1/buf.c
Line	279	279
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/buf.c

Method	translit_text(char *s, int len, int from, int to)

```
....
279.        ctab[i] = i;                /* restore table to initial
state */
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=456
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 273 of ravynos-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	ravynos-1/buf.c	ravynos-1/buf.c
Line	280	280
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ravynos-1/buf.c
Method	translit_text(char *s, int len, int from, int to)

```
....
280.        ctab[i = from] = to;
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=457
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 248 of ravynos-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	ravynos-1/buf.c	ravynos-1/buf.c
Line	267	267
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ravynos-1/buf.c
Method	init_buffers(void)

```
....
267.                ctab[i] = i;
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=458
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 73 of ravynos-1/property.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/property.c	ravynos-1/property.c
Line	130	130
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/property.c
Method	properties_read(int fd)

```
....
130.                    hold_n[n++] = ch;
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=459
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 73 of ravynos-1/property.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/property.c	ravynos-1/property.c
Line	158	158
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/property.c
Method	properties_read(int fd)

```
....
158.                hold_n[n++] = ch;
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=460
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 73 of ravynos-1/property.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/property.c	ravynos-1/property.c
Line	185	185
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/property.c

Method	properties_read(int fd)

```
....
185.                    hold_v[v++] = ch;
```

Char Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=461
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 73 of ravynos-1/property.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/property.c	ravynos-1/property.c
Line	202	202
Object	AssignExpr	AssignExpr

Code Snippet

File Name	ravynos-1/property.c

Method	properties_read(int fd)

```
....
202.                hold_v[v++] = ch;
```

Char Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=462
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 991 of ravynos-1/snprintf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/snprintf.c	ravynos-1/snprintf.c
Line	1034	1034
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/snprintf.c
Method fmtint(char *str, size_t *len, size_t size, INTMAX_T value, int base, int width,

```
....
1034.                   hexprefix = (flags & PRINT_F_UP) ? 'X' : 'x';
```

Char Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=463
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1092 of ravynos-1/snprintf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/snprintf.c	ravynos-1/snprintf.c
Line	1285	1285
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/snprintf.c
Method fmtflt(char *str, size_t *len, size_t size, LDOUBLE fvalue, int width,

```
....
1285.             econvert[epos++] = (flags & PRINT_F_UP) ? 'E' : 'e';
```

Char Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=464
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1076 of ravynos-1/test_x509.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1089	1089
Object	AssignExpr	AssignExpr

Code Snippet
File Name   ravynos-1/test_x509.c
Method   string_to_hash(const char *name)

```
....
1089.                    tmp[v ++] = c;
```

Char Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=465
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1114 of ravynos-1/test_x509.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1127	1127
Object	AssignExpr	AssignExpr

Code Snippet
File Name   ravynos-1/test_x509.c
Method   string_to_curve(const char *name)

```
....
1127.                    tmp[v ++] = c;
```

Char Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=466
Status	New

A variable of a larger data type, map, is being assigned to a smaller data type, in 83 of ravynos-1/name.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	95	95

Object	map	map

Code Snippet
File Name ravynos-1/name.c
Method quote_string(const char *f, size_t len, int flags, size_t *rlen)

```
....
95.    unsigned char map = char_map[from[i]] & flags;
```

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=1070095&projectid=70085&pathid=114
Status	New

The application performs an illegal operation in mtree_atol, in ravynos-1/archive_read_support_format_mtree.c. In line 2032, the program attempts to divide by base, 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 base in mtree_atol of ravynos-1/archive_read_support_format_mtree.c, at line 2032.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	2049	2049
Object	base	base

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method mtree_atol(char **p, int base)

```
....
2049.               limit = INT64_MIN / base;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=115
Status	New

The application performs an illegal operation in mtree_atol, in ravynos-1/archive_read_support_format_mtree.c. In line 2032, the program attempts to divide by base, 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 base in mtree_atol of ravynos-1/archive_read_support_format_mtree.c, at line 2032.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	2050	2050
Object	base	base

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method mtree_atol(char **p, int base)

```
....
2050.                last_digit_limit = -(INT64_MIN % base);
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=116
Status	New

The application performs an illegal operation in mtree_atol, in ravynos-1/archive_read_support_format_mtree.c. In line 2032, the program attempts to divide by base, 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 base in mtree_atol of ravynos-1/archive_read_support_format_mtree.c, at line 2032.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	2063	2063
Object	base	base

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method mtree_atol(char **p, int base)

```
....
2063.                limit = INT64_MAX / base;
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=117
Status	New

The application performs an illegal operation in mtree_atol, in ravynos-1/archive_read_support_format_mtree.c. In line 2032, the program attempts to divide by base, 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 base in mtree_atol of ravynos-1/archive_read_support_format_mtree.c, at line 2032.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	2064	2064
Object	base	base

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method mtree_atol(char **p, int base)

```
....
2064.               last_digit_limit = INT64_MAX % base;
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=118
Status	New

The application performs an illegal operation in update_menuwin, in ravynos-1/menubox.c. In line 325, the program attempts to divide by totnitems, 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 totnitems in update_menuwin of ravynos-1/menubox.c, at line 325.

	Source	Destination
File	ravynos-1/menubox.c	ravynos-1/menubox.c
Line	341	341
Object	totnitems	totnitems

Code Snippet
File Name ravynos-1/menubox.c
Method update_menuwin(struct bsddialog_conf *conf, WINDOW *menuwin, int h, int w,

```
....
341.                    100 * (ymenupad + menurows) / totnitems);
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=119
Status	New

The application performs an illegal operation in ocs_scsi_build_sgls, in ravynos-1/ocs_scsi.c. In line 685, the program attempts to divide by blocksize, 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 blocksize in ocs_scsi_build_sgls of ravynos-1/ocs_scsi.c, at line 685.

	Source	Destination
File	ravynos-1/ocs_scsi.c	ravynos-1/ocs_scsi.c
Line	729	729
Object	blocksize	blocksize

Code Snippet
File Name ravynos-1/ocs_scsi.c
Method ocs_scsi_build_sgls(ocs_hw_t *hw, ocs_hw_io_t *hio, ocs_hw_dif_info_t *hw_dif, ocs_scsi_sgl_t *sgl, uint32_t sgl_count, ocs_hw_io_type_e type)

```
....
729.                    if ((sgl[i].len % blocksize) != 0) {
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=120
Status	New

The application performs an illegal operation in ocs_scsi_build_sgls, in ravynos-1/ocs_scsi.c. In line 685, the program attempts to divide by blocksize, 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 blocksize in ocs_scsi_build_sgls of ravynos-1/ocs_scsi.c, at line 685.

	Source	Destination
File	ravynos-1/ocs_scsi.c	ravynos-1/ocs_scsi.c
Line	752	752
Object	blocksize	blocksize

Code Snippet
File Name ravynos-1/ocs_scsi.c
Method ocs_scsi_build_sgls(ocs_hw_t *hw, ocs_hw_io_t *hio, ocs_hw_dif_info_t *hw_dif, ocs_scsi_sgl_t *sgl, uint32_t sgl_count, ocs_hw_io_type_e type)

```
....
752.                    blockcount = sgl[i].len / blocksize;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=121
Status	New

The application performs an illegal operation in ssl3_write_bytes, in ravynos-1/rec_layer_s3.c. In line 354, the program attempts to divide by split_send_fragment, 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 split_send_fragment in ssl3_write_bytes of ravynos-1/rec_layer_s3.c, at line 354.

	Source	Destination
File	ravynos-1/rec_layer_s3.c	ravynos-1/rec_layer_s3.c
Line	615	615
Object	split_send_fragment	split_send_fragment

Code Snippet

File Name	ravynos-1/rec_layer_s3.c
Method	int ssl3_write_bytes(SSL *s, int type, const void *buf_, size_t len,

```
....
615.            numpipes = ((n - 1) / split_send_fragment) + 1;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=122
Status	New

The application performs an illegal operation in ssl3_write_bytes, in ravynos-1/rec_layer_s3.c. In line 354, the program attempts to divide by numpipes, 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 numpipes in ssl3_write_bytes of ravynos-1/rec_layer_s3.c, at line 354.

	Source	Destination
File	ravynos-1/rec_layer_s3.c	ravynos-1/rec_layer_s3.c
Line	619	619
Object	numpipes	numpipes

Code Snippet

File Name	ravynos-1/rec_layer_s3.c
Method	int ssl3_write_bytes(SSL *s, int type, const void *buf_, size_t len,

```
....
619.          if (n / numpipes >= max_send_fragment) {
```

Divide By Zero\Path 10:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=123
Status	New

The application performs an illegal operation in ssl3_write_bytes, in ravynos-1/rec_layer_s3.c. In line 354, the program attempts to divide by numpipes, 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 numpipes in ssl3_write_bytes of ravynos-1/rec_layer_s3.c, at line 354.

	Source	Destination
File	ravynos-1/rec_layer_s3.c	ravynos-1/rec_layer_s3.c
Line	629	629
Object	numpipes	numpipes

Code Snippet
File Name ravynos-1/rec_layer_s3.c
Method int ssl3_write_bytes(SSL *s, int type, const void *buf_, size_t len,

```
....
629.                tmppipelen = n / numpipes;
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=124
Status	New

The application performs an illegal operation in ssl3_write_bytes, in ravynos-1/rec_layer_s3.c. In line 354, the program attempts to divide by numpipes, 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 numpipes in ssl3_write_bytes of ravynos-1/rec_layer_s3.c, at line 354.

	Source	Destination
File	ravynos-1/rec_layer_s3.c	ravynos-1/rec_layer_s3.c
Line	630	630
Object	numpipes	numpipes

Code Snippet
File Name ravynos-1/rec_layer_s3.c
Method int ssl3_write_bytes(SSL *s, int type, const void *buf_, size_t len,

```
....
630.                remain = n % numpipes;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=125
Status	New

The application performs an illegal operation in report_stats, in ravynos-1/lockstat.c. In line 1753, the program attempts to divide by total_bin_count, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input total_bin_count in report_stats of ravynos-1/lockstat.c, at line 1753.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1922	1922
Object	total_bin_count	total_bin_count

Code Snippet

File Name ravynos-1/lockstat.c

Method report_stats(FILE *out, lsrec_t **sort_buf, size_t nrecs, uint64_t total_count,

```
....
1922.                   uint_t depth = (lsp->ls_hist[j] * 30) /
total_bin_count;
```

Path Traversal

Query Path:

CPP\Cx\CPP Medium Threat\Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description

Path Traversal\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=908
Status	New

Method main at line 3666 of ravynos-1/cxgbetool.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 loadfw at line 1939 of ravynos-1/cxgbetool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	1951
Object	argv	fname

Code Snippet

File Name ravynos-1/cxgbetool.c

Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name ravynos-1/cxgbetool.c

Method loadfw(int argc, const char *argv[])

```
....
1951.        fd = open(fname, O_RDONLY);
```

Path Traversal\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=909
Status	New

Method main at line 3666 of ravynos-1/cxgbetool.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 loadcfg at line 1978 of ravynos-1/cxgbetool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	1993
Object	argv	fname

Code Snippet

File Name ravynos-1/cxgbetool.c

Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name ravynos-1/cxgbetool.c

Method loadcfg(int argc, const char *argv[])

```
....
1993.        fd = open(fname, O_RDONLY);
```

Path Traversal\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=910
Status	New

Method main at line 3666 of ravynos-1/cxgbetool.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 loadboot at line 2085 of ravynos-1/cxgbetool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	2117
Object	argv	fname

Code Snippet
File Name ravynos-1/cxgbetool.c
Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name ravynos-1/cxgbetool.c
Method loadboot(int argc, const char *argv[])

```
....
2117.       fd = open(fname, O_RDONLY);
```

Path Traversal\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=911
Status	New

Method main at line 3666 of ravynos-1/cxgbetool.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 loadbootcfg at line 2144 of ravynos-1/cxgbetool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	2159
Object	argv	fname

Code Snippet
File Name ravynos-1/cxgbetool.c
Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name	ravynos-1/cxgbetool.c
Method	loadbootcfg(int argc, const char *argv[])

```
....
2159.         fd = open(fname, O_RDONLY);
```

Path Traversal\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=912
Status	New

Method main at line 3666 of ravynos-1/cxgbetool.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 dumpstate at line 2021 of ravynos-1/cxgbetool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	2044
Object	argv	fname

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

File Name	ravynos-1/cxgbetool.c
Method	dumpstate(int argc, const char *argv[])

```
....
2044.         fd = open(fname, O_CREAT | O_TRUNC | O_EXCL | O_WRONLY,
```

Path Traversal\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=913
Status	New

Method main at line 3666 of ravynos-1/cxgbetool.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 parse_offload_policy at line 3377 of ravynos-1/cxgbetool.c. This may cause a Path Traversal vulnerability.

	Source	Destination

File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	3386
Object	argv	fname

Code Snippet
File Name ravynos-1/cxgbetool.c
Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name ravynos-1/cxgbetool.c

Method parse_offload_policy(const char *fname, struct t4_offload_policy *op)

```
....
3386.       fp = fopen(fname, "r");
```

Path Traversal\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=914
Status	New

Method main at line 3666 of ravynos-1/cxgbetool.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 real_doit at line 140 of ravynos-1/cxgbetool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	149
Object	argv	buf

Code Snippet
File Name ravynos-1/cxgbetool.c
Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

▼

File Name ravynos-1/cxgbetool.c

Method real_doit(unsigned long cmd, void *data, const char *cmdstr)

```
....
149.            if ((fd = open(buf, O_RDWR)) < 0) {
```

Path Traversal\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=915
Status	New

Method main at line 1744 of ravynos-1/cxgbtool.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 load_fw at line 991 of ravynos-1/cxgbtool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1744	999
Object	argv	fname

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	main(int argc, char *argv[])

```
....
1744.   main(int argc, char *argv[])
```

File Name	ravynos-1/cxgbtool.c
Method	load_fw(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
999.         fd = open(fname, O_RDONLY);
```

Path Traversal\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=916
Status	New

Method main at line 1744 of ravynos-1/cxgbtool.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 load_boot at line 1026 of ravynos-1/cxgbtool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1744	1034
Object	argv	fname

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	main(int argc, char *argv[])

```
....
1744.  main(int argc, char *argv[])
```

▼

File Name	ravynos-1/cxgbtool.c
Method	load_boot(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1034.        fd = open(fname, O_RDONLY);
```

Path Traversal\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=917
Status	New

Method main at line 1744 of ravynos-1/cxgbtool.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 doit at line 128 of ravynos-1/cxgbtool.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1744	136
Object	argv	buf

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	main(int argc, char *argv[])

```
....
1744.  main(int argc, char *argv[])
```

▼

File Name	ravynos-1/cxgbtool.c
Method	doit(const char *iff_name, unsigned long cmd, void *data)

```
....
136.              if ((fd = open(buf, O_RDWR)) < 0)
```

Path Traversal\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=918

Status	New

Method main at line 293 of ravynos-1/phttpget.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 293 of ravynos-1/phttpget.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	293	600
Object	argv	fname

Code Snippet
File Name ravynos-1/phttpget.c
Method main(int argc, char *argv[])

```
....
293.  main(int argc, char *argv[])
....
600.                   fd = open(fname, O_CREAT | O_TRUNC | O_WRONLY,
0644);
```

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=1070095&projectid=70085&pathid=1554
Status	New

The size of the buffer used by SB_set_length in len, at line 171 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	651	175
Object	fgetc	len

Code Snippet
File Name ravynos-1/test_x509.c
Method conf_next_low(void)

```
....
651.                x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_set_length(string_builder *sb, size_t len)

```
....
175.                memset(sb->buf + sb->ptr, ' ', len - sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1555
Status	New

The size of the buffer used by SB_set_length in len, at line 171 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	657	175
Object	fgetc	len

Code Snippet

File Name ravynos-1/test_x509.c

Method conf_next_low(void)

```
....
657.                x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_set_length(string_builder *sb, size_t len)

```
....
175.                memset(sb->buf + sb->ptr, ' ', len - sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1556
Status	New

The size of the buffer used by SB_set_length in BinaryExpr, at line 171 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	651	175
Object	fgetc	BinaryExpr

Code Snippet

File Name ravynos-1/test_x509.c

Method conf_next_low(void)

```
....
651.                    x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_set_length(string_builder *sb, size_t len)

```
....
175.                    memset(sb->buf + sb->ptr, ' ', len - sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1557
Status	New

The size of the buffer used by SB_set_length in BinaryExpr, at line 171 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	657	175
Object	fgetc	BinaryExpr

Code Snippet

File Name ravynos-1/test_x509.c

Method conf_next_low(void)

```
....
657.                    x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_set_length(string_builder *sb, size_t len)

```
....
175.            memset(sb->buf + sb->ptr, ' ', len - sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1558
Status	New

The size of the buffer used by SB_set_length in ptr, at line 171 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	651	175
Object	fgetc	ptr

Code Snippet
File Name ravynos-1/test_x509.c
Method conf_next_low(void)

```
....
651.            x = fgetc(conf);
```

▼

File Name ravynos-1/test_x509.c

Method SB_set_length(string_builder *sb, size_t len)

```
....
175.            memset(sb->buf + sb->ptr, ' ', len - sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1559
Status	New

The size of the buffer used by SB_set_length in ptr, at line 171 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c

Line	657	175
Object	fgetc	ptr

Code Snippet
File Name ravynos-1/test_x509.c
Method conf_next_low(void)

```
....
657.                 x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_set_length(string_builder *sb, size_t len)

```
....
175.                 memset(sb->buf + sb->ptr, ' ', len - sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1560
Status	New

The size of the buffer used by SB_expand in ptr, at line 106 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	651	119
Object	fgetc	ptr

Code Snippet
File Name ravynos-1/test_x509.c
Method conf_next_low(void)

```
....
651.                 x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_expand(string_builder *sb, size_t extra_len)

```
....
119.           memcpy(nbuf, sb->buf, sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1561
Status	New

The size of the buffer used by SB_expand in ptr, at line 106 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	657	119
Object	fgetc	ptr

Code Snippet
File Name ravynos-1/test_x509.c
Method conf_next_low(void)

```
....
657.                x = fgetc(conf);
```

File Name ravynos-1/test_x509.c

Method SB_expand(string_builder *sb, size_t extra_len)

```
....
119.          memcpy(nbuf, sb->buf, sb->ptr);
```

Stored Buffer Overflow boundcpy\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1562
Status	New

The size of the buffer used by eqpkey in key, at line 1408 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_all passes to BinaryExpr, at line 403 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	423	1429
Object	BinaryExpr	key

Code Snippet
File Name ravynos-1/test_x509.c

Method read_all(FILE *f, size_t *len)

```
....
423.            rlen = fread(buf + ptr, 1, blen - ptr, f);
```

File Name ravynos-1/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1429.                        pk2->key.ec.q, pk1->key.ec.qlen) == 0;
```

Long Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Long 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

Long Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=486
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 550 of ravynos-1/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c
Line	553	553
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/b_print.c
Method static long roundv(LDOUBLE value)

```
....
553.     intpart = (long)value;
```

Long Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=487

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 561 of ravynos-1/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/b_print.c	ravynos-1/b_print.c
Line	663	663
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/b_print.c
Method fmtfp(char **sbuffer,

```
....
663.       intpart = (unsigned long)ufvalue;
```

Long Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=488
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 652 of ravynos-1/bsd-snprintf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/bsd-snprintf.c	ravynos-1/bsd-snprintf.c
Line	656	656
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/bsd-snprintf.c
Method static LLONG ROUND(LDOUBLE value)

```
....
656.         intpart = (LLONG)value;
```

Long Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=489
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 665 of ravynos-1/bsd-snprintf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ravynos-1/bsd-snprintf.c	ravynos-1/bsd-snprintf.c
Line	673	673
Object	AssignExpr	AssignExpr

Code Snippet
File Name ravynos-1/bsd-snprintf.c
Method static double my_modf(double x0, double *iptr)

```
....
673.                  l = (long)x;
```

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=1070095&projectid=70085&pathid=1551
Status	New

The function malloc in ravynos-1/mrsas.c at line 2324 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	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	2429	2429
Object	sizeof	malloc

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_init_fw(struct mrsas_softc *sc)

```
....
2429.       sc->ctrl_info = malloc(sizeof(struct mrsas_ctrl_info),
M_MRSAS, M_NOWAIT);
```

Wrong Memory Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=1552
Status	New

The function malloc in ravynos-1/mrsas.c at line 2324 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	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	2488	2488
Object	sizeof	malloc

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_init_fw(struct mrsas_softc *sc)

```
....
2488.                        sc->streamDetectByLD[i] = 
malloc(sizeof(LD_STREAM_DETECT), M_MRSAS, M_NOWAIT);
```

Wrong Memory Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1553
Status	New

The function malloc in ravynos-1/property.c at line 47 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	ravynos-1/property.c	ravynos-1/property.c
Line	51	51
Object	sizeof	malloc

Code Snippet
File Name ravynos-1/property.c
Method property_alloc(char *name, char *value)

```
....
51.       if ((n = (properties)malloc(sizeof(struct _property))) == NULL)
```

Stored Buffer Overflow cpycat

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow cpycat Version:0

Categories

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

Description

Stored Buffer Overflow cpycat\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1563
Status	New

The size of the buffer used by my_popen in command, at line 67 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_cpuid_set passes to linebuf, at line 2334 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2510	92
Object	linebuf	command

Code Snippet

File Name ravynos-1/pmcstudy.c

Method get_cpuid_set(void)

```
....
2510.       while (fgets(linebuf, sizeof(linebuf), io) != NULL) {
```

File Name ravynos-1/pmcstudy.c

Method my_popen(const char *command, const char *dir, pid_t *p_pid)

```
....
92.   strcpy(cmd2, command);
```

Stored Buffer Overflow cpycat\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1564
Status	New

The size of the buffer used by process_header in Address, at line 2064 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that build_counters_from_header passes to buffer, at line 2095 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2104	2086
Object	buffer	Address

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	build_counters_from_header(FILE *io)

```
....
2104.        if (fgets(buffer, sizeof(buffer), io) == NULL) {
```

▼

File Name	ravynos-1/pmcstudy.c
Method	process_header(int idx, char *p)

```
....
2086.                              strcpy(up->counter_name, &p[(i+1)]);
```

Stored Buffer Overflow cpycat\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1565
Status	New

The size of the buffer used by process_header in p, at line 2064 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that build_counters_from_header passes to buffer, at line 2095 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2104	2086
Object	buffer	p

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	build_counters_from_header(FILE *io)

```
....
2104.        if (fgets(buffer, sizeof(buffer), io) == NULL) {
```

▼

File Name	ravynos-1/pmcstudy.c
Method	process_header(int idx, char *p)

```
....
2086.                              strcpy(up->counter_name, &p[(i+1)]);
```

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=1070095&projectid=70085&pathid=126
Status	New

The pointer chacha20 at ravynos-1/e_chacha20_poly1305.c in line 143 is being used after it has been freed.

	Source	Destination
File	ravynos-1/e_chacha20_poly1305.c	ravynos-1/e_chacha20_poly1305.c
Line	145	145
Object	chacha20	chacha20

Code Snippet
File Name ravynos-1/e_chacha20_poly1305.c
Method const EVP_CIPHER *EVP_chacha20(void)

```
....
145.        return &chacha20;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=127
Status	New

The pointer rand_chan at ravynos-1/acs.c in line 838 is being used after it has been freed.

	Source	Destination
File	ravynos-1/acs.c	ravynos-1/acs.c
Line	899	899
Object	rand_chan	rand_chan

Code Snippet
File Name ravynos-1/acs.c
Method acs_find_ideal_chan(struct hostapd_iface *iface)

```
....
899.          return rand_chan;
```

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=1070095&projectid=70085&pathid=919
Status	New

Method shadow_pw at line 129 of ravynos-1/xcrypt.c defines pw_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pw_password, this variable is never cleared from memory.

	Source	Destination
File	ravynos-1/xcrypt.c	ravynos-1/xcrypt.c
Line	131	131
Object	pw_password	pw_password

Code Snippet
File Name ravynos-1/xcrypt.c
Method shadow_pw(struct passwd *pw)

```
....
131.        char *pw_password = pw->pw_passwd;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=920
Status	New

Method pick_salt at line 71 of ravynos-1/xcrypt.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	ravynos-1/xcrypt.c	ravynos-1/xcrypt.c
Line	74	74
Object	passwd	passwd

Code Snippet	
File Name	ravynos-1/xcrypt.c
Method	pick_salt(void)

```
....
74.    char *passwd, *p;
```

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=1070095&projectid=70085&pathid=1004
Status	New

The variable declared in peer at ravynos-1/show.c in line 47 is not initialized when it is used by peer at ravynos-1/show.c in line 47.

	Source	Destination
File	ravynos-1/show.c	ravynos-1/show.c
Line	50	60
Object	peer	peer

Code Snippet	
File Name	ravynos-1/show.c
Method	static void sort_peers(struct wgdevice *device)

```
....
50.    struct wgpeer *peer, **peers;
....
60.            peers[i++] = peer;
```

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=1070095&projectid=70085&pathid=1187
Status	New

The variable declared in null at ravynos-1/archive_read_support_format_mtree.c in line 887 is not initialized when it is used by value at ravynos-1/archive_read_support_format_mtree.c in line 835.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	909	853
Object	null	value

Code Snippet

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	process_global_unset(struct archive_read *a,

```
....
909.                    *global = NULL;
```

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	remove_option(struct mtree_option **global, const char *value, size_t len)

```
....
853.          free(iter->value);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1188
Status	New

The variable declared in null at ravynos-1/archive_read_support_format_mtree.c in line 1175 is not initialized when it is used by st_mtimespec at ravynos-1/archive_read_support_format_mtree.c in line 1175.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1284	1363
Object	null	st_mtimespec

Code Snippet

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	parse_file(struct archive_read *a, struct archive_entry *entry,

```
....
1284.                     st = NULL;
....
1363.                                         st->st_mtimespec.tv_nsec);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1189
Status	New

The variable declared in null at ravynos-1/archive_read_support_format_mtree.c in line 1175 is not initialized when it is used by st_mtimespec at ravynos-1/archive_read_support_format_mtree.c in line 1175.

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1281	1363
Object	null	st_mtimespec

Code Snippet

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	parse_file(struct archive_read *a, struct archive_entry *entry,

```
....
1281.                           st = NULL;
....
1363.                                         st->st_mtimespec.tv_nsec);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1190
Status	New

The variable declared in null at ravynos-1/authzone.c in line 7689 is not initialized when it is used by Pointer at ravynos-1/authzone.c in line 1875.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7695	1947
Object	null	Pointer

Code Snippet

File Name	ravynos-1/authzone.c

Method	int auth_zone_generate_zonemd_check(struct auth_zone* z, int scheme,

```
....
7695.        *reason = NULL;
```

File Name	ravynos-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=1070095&projectid=70085&pathid=1191
Status	New

The variable declared in null at ravynos-1/authzone.c in line 1875 is not initialized when it is used by Pointer at ravynos-1/authzone.c in line 1875.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1936	1947
Object	null	Pointer

Code Snippet

File Name	ravynos-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 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1192
Status	New

The variable declared in null at ravynos-1/authzone.c in line 7995 is not initialized when it is used by Pointer at ravynos-1/authzone.c in line 1875.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7999	1947
Object	null	Pointer

Code Snippet
File Name ravynos-1/authzone.c
Method auth_zone_verify_zonemd_with_key(struct auth_zone* z, struct module_env* env,

```
....
7999.        char* reason = NULL, *why_bogus = NULL;
```

File Name ravynos-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 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1193
Status	New

The variable declared in null at ravynos-1/authzone.c in line 2094 is not initialized when it is used by task_transfer at ravynos-1/authzone.c in line 2094.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	2097	2169
Object	null	task_transfer

Code Snippet
File Name ravynos-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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1194
Status	New

The variable declared in null at ravynos-1/authzone.c in line 2094 is not initialized when it is used by task_probe at ravynos-1/authzone.c in line 2094.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	2097	2164
Object	null	task_probe

Code Snippet

File Name	ravynos-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 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1195
Status	New

The variable declared in null at ravynos-1/authzone.c in line 3558 is not initialized when it is used by rep at ravynos-1/authzone.c in line 3515.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3562	3527
Object	null	rep

Code Snippet

File Name	ravynos-1/authzone.c
Method	int auth_zones_answer(struct auth_zones* az, struct module_env* env,

```
....
3562.         struct dns_msg* msg = NULL;
```

File Name ravynos-1/authzone.c

Method auth_answer_encode(struct query_info* qinfo, struct module_env* env,

```
....
3527.             (int)FLAGS_GET_RCODE(msg->rep->flags), edns, repinfo,
temp, env->now_tv)
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1196
Status	New

The variable declared in null at ravynos-1/authzone.c in line 3966 is not initialized when it is used by task_probe at ravynos-1/authzone.c in line 6312.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3968	6318
Object	null	task_probe

Code Snippet

File Name ravynos-1/authzone.c

Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3968.       struct auth_master* list = NULL, *last = NULL;
```

File Name ravynos-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6318.       comm_point_delete(xfr->task_probe->cp);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1197
Status	New

The variable declared in null at ravynos-1/authzone.c in line 3966 is not initialized when it is used by task_probe at ravynos-1/authzone.c in line 6312.

	Source	Destination

File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3968	6315
Object	null	task_probe

Code Snippet
File Name ravynos-1/authzone.c
Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3968.        struct auth_master* list = NULL, *last = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_probe_disown(struct auth_xfer* xfr)

```
....
6315.        comm_timer_delete(xfr->task_probe->timer);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1198
Status	New

The variable declared in null at ravynos-1/authzone.c in line 3966 is not initialized when it is used by task_probe at ravynos-1/authzone.c in line 4130.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3968	4132
Object	null	task_probe

Code Snippet
File Name ravynos-1/authzone.c
Method probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3968.        struct auth_master* list = NULL, *last = NULL;
```

▼

File Name ravynos-1/authzone.c

Method xfr_probe_end_of_list(struct auth_xfer* xfr)

```
....
4132.       return !xfr->task_probe->scan_specific && !xfr->task_probe-
>scan_target;
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1199
Status	New

The variable declared in null at ravynos-1/authzone.c in line 3966 is not initialized when it is used by task_probe at ravynos-1/authzone.c in line 4130.

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3968	4132
Object	null	task_probe

Code Snippet

File Name	ravynos-1/authzone.c
Method	probe_copy_masters_for_allow_notify(struct auth_xfer* xfr)

```
....
3968.       struct auth_master* list = NULL, *last = NULL;
```

File Name	ravynos-1/authzone.c
Method	xfr_probe_end_of_list(struct auth_xfer* xfr)

```
....
4132.       return !xfr->task_probe->scan_specific && !xfr->task_probe-
>scan_target;
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1200
Status	New

The variable declared in null at ravynos-1/channels.c in line 640 is not initialized when it is used by host_to_connect at ravynos-1/channels.c in line 640.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c

Line	656	656
Object	null	host_to_connect

Code Snippet
File Name ravynos-1/channels.c
Method permission_set_add(struct ssh *ssh, int who, int where,

```
....
656.		(*permp)[n].host_to_connect = MAYBE_DUP(host_to_connect);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1201
Status	New

The variable declared in null at ravynos-1/channels.c in line 640 is not initialized when it is used by listen_host at ravynos-1/channels.c in line 640.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	658	658
Object	null	listen_host

Code Snippet
File Name ravynos-1/channels.c
Method permission_set_add(struct ssh *ssh, int who, int where,

```
....
658.		(*permp)[n].listen_host = MAYBE_DUP(listen_host);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1202
Status	New

The variable declared in null at ravynos-1/channels.c in line 640 is not initialized when it is used by listen_path at ravynos-1/channels.c in line 640.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	659	659
Object	null	listen_path

Code Snippet

File Name	ravynos-1/channels.c
Method	permission_set_add(struct ssh *ssh, int who, int where,

```
....
659.        (*permp)[n].listen_path = MAYBE_DUP(listen_path);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1203
Status	New

The variable declared in null at ravynos-1/channels.c in line 3721 is not initialized when it is used by listening_addr at ravynos-1/channels.c in line 3721.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3864	3864
Object	null	listening_addr

Code Snippet

File Name	ravynos-1/channels.c
Method	channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3864.           c->listening_addr = addr == NULL ? NULL :
xstrdup(addr);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1204
Status	New

The variable declared in 0 at ravynos-1/channels.c in line 3721 is not initialized when it is used by listening_port at ravynos-1/channels.c in line 3721.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3776	3867
Object	0	listening_port

Code Snippet

File Name	ravynos-1/channels.c
Method	channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3776.                *allocated_listen_port = 0;
....
3867.                      c->listening_port = *allocated_listen_port;
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1205
Status	New

The variable declared in null at ravynos-1/channels.c in line 4085 is not initialized when it is used by listening_port at ravynos-1/channels.c in line 3721.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	4093	3867
Object	null	listening_port

Code Snippet

File Name	ravynos-1/channels.c
Method	channel_setup_local_fwd_listener(struct ssh *ssh,

```
....
4093.                     SSH_CHANNEL_PORT_LISTENER, fwd, NULL, fwd_opts);
```

File Name	ravynos-1/channels.c
Method	channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3867.                      c->listening_port = *allocated_listen_port;
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1206
Status	New

The variable declared in null at ravynos-1/ec_asn1.c in line 585 is not initialized when it is used by seed at ravynos-1/ec_asn1.c in line 585.

	Source	Destination

File	ravynos-1/ec_asn1.c	ravynos-1/ec_asn1.c
Line	588	764
Object	null	seed

Code Snippet
File Name ravynos-1/ec_asn1.c
Method EC_GROUP *EC_GROUP_new_from_ecparameters(const ECPARAMETERS *params)

```
....
588.        EC_GROUP *ret = NULL, *dup = NULL;
....
764.            OPENSSL_free(ret->seed);
```

NULL Pointer Dereference\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1207
Status New

The variable declared in null at ravynos-1/ec_asn1.c in line 985 is not initialized when it is used by value at ravynos-1/ec_asn1.c in line 532.

	Source	Destination
File	ravynos-1/ec_asn1.c	ravynos-1/ec_asn1.c
Line	988	545
Object	null	value

Code Snippet
File Name ravynos-1/ec_asn1.c
Method int i2d_ECPKParameters(const EC_GROUP *a, unsigned char **out)

```
....
988.        ECPKPARAMETERS *tmp = EC_GROUP_get_ecpkparameters(a, NULL);
```

File Name ravynos-1/ec_asn1.c
Method ECPKPARAMETERS *EC_GROUP_get_ecpkparameters(const EC_GROUP *group,

```
....
545.                ASN1_OBJECT_free(ret->value.named_curve);
```

NULL Pointer Dereference\Path 22:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1208
Status	New

The variable declared in null at ravynos-1/ec_asn1.c in line 985 is not initialized when it is used by value at ravynos-1/ec_asn1.c in line 532.

	Source	Destination
File	ravynos-1/ec_asn1.c	ravynos-1/ec_asn1.c
Line	988	548
Object	null	value

Code Snippet

File Name ravynos-1/ec_asn1.c

Method int i2d_ECPKParameters(const EC_GROUP *a, unsigned char **out)

```
....
988.      ECPKPARAMETERS *tmp = EC_GROUP_get_ecpkparameters(a, NULL);
```

File Name ravynos-1/ec_asn1.c

Method ECPKPARAMETERS *EC_GROUP_get_ecpkparameters(const EC_GROUP *group,

```
....
548.              ECPARAMETERS_free(ret->value.parameters);
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1209
Status	New

The variable declared in null at ravynos-1/ec_asn1.c in line 985 is not initialized when it is used by value at ravynos-1/ec_asn1.c in line 532.

	Source	Destination
File	ravynos-1/ec_asn1.c	ravynos-1/ec_asn1.c
Line	988	547
Object	null	value

Code Snippet

File Name ravynos-1/ec_asn1.c

Method int i2d_ECPKParameters(const EC_GROUP *a, unsigned char **out)

```
....
988.      ECPKPARAMETERS *tmp = EC_GROUP_get_ecpkparameters(a, NULL);
```

File Name	ravynos-1/ec_asn1.c
Method	ECPKPARAMETERS *EC_GROUP_get_ecpkparameters(const EC_GROUP *group,

```
....
547.                       && ret->value.parameters != NULL)
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1210
Status	New

The variable declared in null at ravynos-1/krb5_mech.c in line 1399 is not initialized when it is used by m_len at ravynos-1/krb5_mech.c in line 1399.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1448	1532
Object	null	m_len

Code Snippet

File Name	ravynos-1/krb5_mech.c
Method	krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1448.                       tm = NULL;
....
1532.               tm->m_len -= 16;
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1211
Status	New

The variable declared in null at ravynos-1/krb5_mech.c in line 1399 is not initialized when it is used by m_data at ravynos-1/krb5_mech.c in line 1399.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1448	1529
Object	null	m_data

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1448.                   tm = NULL;
....
1529.             bcopy(p, tm->m_data, 16);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1212
Status	New

The variable declared in null at ravynos-1/krb5_mech.c in line 1399 is not initialized when it is used by m_data at ravynos-1/krb5_mech.c in line 1399.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1448	1531
Object	null	m_data

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1448.                   tm = NULL;
....
1531.             tm->m_data += 16;
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1213
Status	New

The variable declared in null at ravynos-1/sctp_sys_calls.c in line 877 is not initialized when it is used by recvv_rcvinfo at ravynos-1/sctp_sys_calls.c in line 877.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	921	949
Object	null	recvv_rcvinfo

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_recvv(int sd,

```
....
921.            rcvinfo = NULL;
....
949.                    rn_info->recvv_rcvinfo = *rcvinfo;
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1214
Status	New

The variable declared in null at ravynos-1/sctp_sys_calls.c in line 877 is not initialized when it is used by recvv_nxtinfo at ravynos-1/sctp_sys_calls.c in line 877.

	Source	Destination
File	ravynos-1/sctp_sys_calls.c	ravynos-1/sctp_sys_calls.c
Line	922	950
Object	null	recvv_nxtinfo

Code Snippet
File Name ravynos-1/sctp_sys_calls.c
Method sctp_recvv(int sd,

```
....
922.            nxtinfo = NULL;
....
950.                    rn_info->recvv_nxtinfo = *nxtinfo;
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1215
Status	New

The variable declared in null at ravynos-1/servconf.c in line 883 is not initialized when it is used by rdomain at ravynos-1/servconf.c in line 883.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	895	895
Object	null	rdomain

Code Snippet
File Name ravynos-1/servconf.c
Method queue_listen_addr(ServerOptions *options, const char *addr,

```
....
895.         qla->rdomain = rdomain == NULL ? NULL : xstrdup(rdomain);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1216
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by host at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1189
Object	null	host

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                 (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c
Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1189.                   if (ci->host == NULL)
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1217
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by host at ravynos-1/servconf.c in line 1118.

	Source	Destination

File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1128
Object	null	host

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                 (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

▼

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1128.                 ci->host ? ci->host : "(null)",
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1218
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by host at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1128
Object	null	host

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                 (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

▼

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1128.                    ci->host ? ci->host : "(null)",
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1219
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by address at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1209
Object	null	address

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                    (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1209.                                "%.100s' at line %d", ci->address,
arg, line);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1220
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by addr_match_list at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c

Line	2258	1206
Object	null	addr_match_list

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1206.                    switch (addr_match_list(ci->address, arg)) {
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1221
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by address at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1204
Object	null	address

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1204.                    if (ci->address == NULL)
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1222
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by address at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1129
Object	null	address

Code Snippet

File Name ravynos-1/servconf.c

Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                    (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1129.                   ci->address ? ci->address : "(null)",
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1223
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by address at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1129
Object	null	address

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1129.                ci->address ? ci->address : "(null)",
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1224
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by laddress at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1234
Object	null	laddress

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1234.                            ci->laddress, arg, line);
```

NULL Pointer Dereference\Path 39:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1225
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by addr_match_list at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1230
Object	null	addr_match_list

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1230.                  switch (addr_match_list(ci->laddress, arg)) {
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1226
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by laddress at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1227
Object	null	laddress

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                    (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

▼

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1227.                      if (ci->laddress == NULL)
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1227
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by laddress at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1130
Object	null	laddress

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                    (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

▼

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1130.                    ci->laddress ? ci->laddress : "(null)", ci-
>lport);
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=1228
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by laddress at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1130
Object	null	laddress

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                  (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c
Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1130.                  ci->laddress ? ci->laddress : "(null)", ci-
>lport);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1229
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by lport at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1130
Object	null	lport

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                 (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

▼

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1130.                 ci->laddress ? ci->laddress : "(null)", ci-
>lport);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1230
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by rdomain at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1267
Object	null	rdomain

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                 (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

▼

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1267.                   if (ci->rdomain == NULL)
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=1231
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by user at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1164
Object	null	user

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                   (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1164.                     if (ci->user == NULL)
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1232
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by match_cfg_line_group at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1178
Object	null	match_cfg_line_group

Code Snippet
File Name ravynos-1/servconf.c
Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1178.                  switch (match_cfg_line_group(arg, line, ci-
>user)) {
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1233
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by user at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1176
Object	null	user

Code Snippet

File Name	ravynos-1/servconf.c
Method	process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name	ravynos-1/servconf.c
Method	match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1176.                  if (ci->user == NULL)
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=1234
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by user at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1127
Object	null	user

Code Snippet

File Name ravynos-1/servconf.c

Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                   (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1127.                   "laddr %s lport %d", cp, ci->user ? ci->user :
"(null)",
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1235
Status	New

The variable declared in null at ravynos-1/servconf.c in line 1345 is not initialized when it is used by user at ravynos-1/servconf.c in line 1118.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2258	1127
Object	null	user

Code Snippet

File Name ravynos-1/servconf.c

Method process_server_config_line_depth(ServerOptions *options, char *line,

```
....
2258.                (*inc_flags & SSHCFG_NEVERMATCH ? NULL :
connectinfo));
```

▼

File Name ravynos-1/servconf.c

Method match_cfg_line(char **condition, int line, struct connection_info *ci)

```
....
1127.                "laddr %s lport %d", cp, ci->user ? ci->user :
"(null)",
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1236
Status	New

The variable declared in null at ravynos-1/show.c in line 379 is not initialized when it is used by public_key at ravynos-1/show.c in line 253.

	Source	Destination
File	ravynos-1/show.c	ravynos-1/show.c
Line	440	261
Object	null	public_key

Code Snippet

File Name ravynos-1/show.c

Method int show_main(int argc, const char *argv[])

```
....
440.            struct wgdevice *device = NULL;
```

▼

File Name ravynos-1/show.c

Method static void dump_print(struct wgdevice *device, bool with_interface)

```
....
261.        printf("%s\t", maybe_key(device->public_key, device->flags &
WGDEVICE_HAS_PUBLIC_KEY));
```

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=1070095&projectid=70085&pathid=1566
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3626	3626
Object	fgets	fgets

Code Snippet
File Name ravynos-1/cxgbetool.c
Method run_cmd_loop(void)

```
....
3626.                buf = fgets(buffer, sizeof(buffer), stdin);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1567
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	249	249
Object	fgets	fgets

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
249.         while ((fgets(buf, BUFSIZ, tmp)) != NULL) {
```

Improper Resource Access Authorization\Path 3:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1568
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1136	1136
Object	fgets	fgets

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_resetconfig(int argc, char * const *argv)

```
....
1136.               fgets(reply, sizeof(reply), stdin);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1569
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2104	2104
Object	fgets	fgets

Code Snippet
File Name ravynos-1/pmcstudy.c
Method build_counters_from_header(FILE *io)

```
....
2104.         if (fgets(buffer, sizeof(buffer), io) == NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1570
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2160	2160

Object	fgets	fgets

Code Snippet
File Name ravynos-1/pmcstudy.c
Method read_a_line(FILE *io)

```
....
2160.        if (fgets(buffer, sizeof(buffer), io) == NULL) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1571
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2510	2510
Object	fgets	fgets

Code Snippet
File Name ravynos-1/pmcstudy.c
Method get_cpuid_set(void)

```
....
2510.        while (fgets(linebuf, sizeof(linebuf), io) != NULL) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1572
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2591	2591
Object	fgets	fgets

Code Snippet
File Name ravynos-1/pmcstudy.c
Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2591.        if (fgets(line, sizeof(line), io) == NULL) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1573
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2607	2607
Object	fgets	fgets

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2607.                if (fgets(line, sizeof(line), io) == NULL) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1574
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	651	651
Object	fgetc	fgetc

Code Snippet

File Name	ravynos-1/test_x509.c
Method	conf_next_low(void)

```
....
651.              x = fgetc(conf);
```

Improper Resource Access Authorization\Path 10:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1575
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	657	657
Object	fgetc	fgetc

Code Snippet
File Name ravynos-1/test_x509.c
Method conf_next_low(void)

```
....
657.                x = fgetc(conf);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1576
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3626	3626
Object	buffer	buffer

Code Snippet
File Name ravynos-1/cxgbetool.c
Method run_cmd_loop(void)

```
....
3626.               buf = fgets(buffer, sizeof(buffer), stdin);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1577
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	249	249

Object	buf	buf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
249.        while ((fgets(buf, BUFSIZ, tmp)) != NULL) {
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1578
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1136	1136
Object	reply	reply

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_resetconfig(int argc, char * const *argv)

```
....
1136.           fgets(reply, sizeof(reply), stdin);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1579
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2104	2104
Object	buffer	buffer

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	build_counters_from_header(FILE *io)

```
....
2104.        if (fgets(buffer, sizeof(buffer), io) == NULL) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1580
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2160	2160
Object	buffer	buffer

Code Snippet
File Name ravynos-1/pmcstudy.c
Method read_a_line(FILE *io)

```
....
2160.        if (fgets(buffer, sizeof(buffer), io) == NULL) {
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1581
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2510	2510
Object	linebuf	linebuf

Code Snippet
File Name ravynos-1/pmcstudy.c
Method get_cpuid_set(void)

```
....
2510.        while (fgets(linebuf, sizeof(linebuf), io) != NULL) {
```

Improper Resource Access Authorization\Path 17:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1582
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2591	2591
Object	line	line

Code Snippet
File Name ravynos-1/pmcstudy.c
Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2591.        if (fgets(line, sizeof(line), io) == NULL) {
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1583
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2607	2607
Object	line	line

Code Snippet
File Name ravynos-1/pmcstudy.c
Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2607.                    if (fgets(line, sizeof(line), io) == NULL) {
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1584
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	67	67

Object	sfbuf	sfbuf

Code Snippet
File Name ravynos-1/buf.c
Method get_sbuf_line(line_t *lp)

```
....
67.    if (fread(sfbuf, sizeof(char), len, sfp) != len) {
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1585
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	423	423
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ravynos-1/test_x509.c
Method read_all(FILE *f, size_t *len)

```
....
423.                rlen = fread(buf + ptr, 1, blen - ptr, f);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1586
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1904	1904
Object	buff	buff

Code Snippet
File Name ravynos-1/archive_read_support_format_mtree.c
Method read_data(struct archive_read *a, const void **buff, size_t *size,

```
....
1904.        bytes_read = read(mtree->fd, mtree->buff, bytes_to_read);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1587
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2098	2098
Object	buf	buf

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

```
....
2098.        len = read(c->rfd, buf, sizeof(buf));
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1588
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2266	2266
Object	buf	buf

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

```
....
2266.        len = read(c->efd, buf, sizeof(buf));
```

Improper Resource Access Authorization\Path 24:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1589
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2348	2348
Object	buf	buf

Code Snippet
File Name ravynos-1/channels.c
Method read_mux(struct ssh *ssh, Channel *c, u_int need)

```
....
2348.                len = read(c->rfd, buf, MINIMUM(rlen, CHAN_RBUF));
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1590
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1008	1008
Object	buf	buf

Code Snippet
File Name ravynos-1/cxgbtool.c
Method load_fw(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1008.        len = read(fd, op.buf, MAX_FW_IMAGE_SIZE + 1);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1591
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1042	1042

Object	buf	buf

Code Snippet
File Name ravynos-1/cxgbtool.c
Method load_boot(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1042.        len = read(fd, op.buf, MAX_BOOT_IMAGE_SIZE + 1);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1592
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1715	1715
Object	buf	buf

Code Snippet
File Name ravynos-1/cxgbtool.c
Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1715.                n = read(STDIN_FILENO, buf, sizeof(buf) - 1);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1593
Status	New

	Source	Destination
File	ravynos-1/property.c	ravynos-1/property.c
Line	96	96
Object	buf	buf

Code Snippet
File Name ravynos-1/property.c
Method properties_read(int fd)

```
....
96.        if ((max = read(fd, buf, sizeof buf)) < 0) {
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1594
Status	New

	Source	Destination
File	ravynos-1/query.c	ravynos-1/query.c
Line	1195	1195
Object	buf	buf

Code Snippet
File Name ravynos-1/query.c
Method query_socket_read(struct query_state *qstate, void *buf, size_t nbytes)

```
....
1195.        result = read(qstate->sockfd, buf, nbytes);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1595
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	60	60
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method get_sbuf_line(line_t *lp)

```
....
60.                fprintf(stderr, "%s\n", strerror(errno));
```

Improper Resource Access Authorization\Path 31:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1596
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	68	68
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method get_sbuf_line(line_t *lp)

```
....
68.          fprintf(stderr, "%s\n", strerror(errno));
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1597
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	88	88
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method put_sbuf_line(const char *cs)

```
....
88.          fprintf(stderr, "%s\n", strerror(errno));
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1598
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	104	104

Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method put_sbuf_line(const char *cs)

```
....
104.                    fprintf(stderr, "%s\n", strerror(errno));
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1599
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	115	115
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method put_sbuf_line(const char *cs)

```
....
115.              fprintf(stderr, "%s\n", strerror(errno));
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1600
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	220	220
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method close_sbuf(void)

```
....
220.                fprintf(stderr, "%s: %s\n", sfn,
strerror(errno));
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1601
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	93	93
Object	fprintf	fprintf

Code Snippet

File Name ravynos-1/cxgbetool.c

Method usage(FILE *fp)

```
....
93.    fprintf(fp, "Usage: %s <nexus> [operation]\n", progname);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1602
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	94	94
Object	fprintf	fprintf

Code Snippet

File Name ravynos-1/cxgbetool.c

Method usage(FILE *fp)

```
....
94.    fprintf(fp,
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1603
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	313	313
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/cxgbetool.c
Method dump_regs_table(int argc, const char *argv[], const uint32_t *regs,

```
....
313.                        fprintf(stderr, "\nAvailable blocks:");
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1604
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	315	315
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/cxgbetool.c
Method dump_regs_table(int argc, const char *argv[], const uint32_t *regs,

```
....
315.                              fprintf(stderr, " %s", modtab->name);
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1605
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c

Line	316	316
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/cxgbetool.c
Method dump_regs_table(int argc, const char *argv[], const uint32_t *regs,

```
....
316.                    fprintf(stderr, "\n");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1606
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3624	3624
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/cxgbetool.c
Method run_cmd_loop(void)

```
....
3624.           fprintf(stdout, "> ");
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1607
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	91	91
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/cxgbtool.c
Method usage(FILE *fp)

```
....
91.    fprintf(fp, "Usage: %s <interface> [operation]\n", progname);
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1608
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	92	92
Object	fprintf	fprintf

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	usage(FILE *fp)

```
....
92.    fprintf(fp,
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1609
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1713	1713
Object	fprintf	fprintf

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1713.             fprintf(stdout, "> ");
```

Improper Resource Access Authorization\Path 45:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1610
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1444	1444
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method printconfig(FILE *of, const char *comment)

```
....
1444.        fprintf(of, "# Vinum configuration of %s, saved at %s",
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1611
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1449	1449
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method printconfig(FILE *of, const char *comment)

```
....
1449.            fprintf(of, "# Current configuration:\n");
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1612
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1451	1451

Object	fprintf	fprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	printconfig(FILE *of, const char *comment)

```
....
1451.        fprintf(of, "%s", buf);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1613
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	179	179
Object	fprintf	fprintf

Code Snippet

File Name	ravynos-1/http.c
Method	http_new_chunk(struct httpio *io)

```
....
179.                    fprintf(stderr, "%s(): end of last chunk\n",
__func__);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1614
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	181	181
Object	fprintf	fprintf

Code Snippet

File Name	ravynos-1/http.c
Method	http_new_chunk(struct httpio *io)

```
....
181.                fprintf(stderr, "%s(): new chunk: %lu (%lu)\n",
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1615
Status	New

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1963	1963
Object	fprintf	fprintf

Code Snippet
File Name ravynos-1/lockstat.c
Method report_trace(FILE *out, lsrec_t **sort_buf)

```
....
1963.           (void) fprintf(out, "%5s  %7s  %11s  %-24s  %-24s\n",
```

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=1070095&projectid=70085&pathid=1041
Status	New

The archive_read_format_lha_read_header method calls the snprintf function, at line 475 of ravynos-1/archive_read_support_format_lha.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	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	742	742
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method archive_read_format_lha_read_header(struct archive_read *a,

```
....
742.        snprintf(lha->format_name, sizeof(lha->format_name), "lha -
%c%c%c-",
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1042
Status	New

The auth_zone_generate_answer method calls the snprintf function, at line 3425 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3455	3455
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/authzone.c
Method auth_zone_generate_answer(struct auth_zone* z, struct query_info* qinfo,

```
....
3455.             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=1070095&projectid=70085&pathid=1043
Status	New

The auth_zone_generate_answer method calls the snprintf function, at line 3425 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3459	3459
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/authzone.c
Method auth_zone_generate_answer(struct auth_zone* z, struct query_info* qinfo,

```
....
3459.             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=1070095&projectid=70085&pathid=1044
Status	New

The auth_zone_generate_answer method calls the snprintf function, at line 3425 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	3462	3462
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/authzone.c
Method auth_zone_generate_answer(struct auth_zone* z, struct query_info* qinfo,

```
....
3462.             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=1070095&projectid=70085&pathid=1045
Status	New

The xfr_write_after_update method calls the snprintf function, at line 5165 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5210	5210
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_write_after_update(struct auth_xfer* xfr, struct module_env* env)

```
....
5210.       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=1070095&projectid=70085&pathid=1046
Status New

The xfr_transfer_lookup_host method calls the snprintf function, at line 5374 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5411	5411
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_transfer_lookup_host(struct auth_xfer* xfr, struct module_env* env)

```
....
5411.             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=1070095&projectid=70085&pathid=1047
Status New

The xfr_probe_lookup_host method calls the snprintf function, at line 6565 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	6604	6604
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/authzone.c
Method xfr_probe_lookup_host(struct auth_xfer* xfr, struct module_env* env)

```
....
6604.          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=1070095&projectid=70085&pathid=1048
Status	New

The auth_zone_zonemd_fail method calls the snprintf function, at line 7947 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	7958	7958
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/authzone.c
Method static void auth_zone_zonemd_fail(struct auth_zone* z, struct module_env* env,

```
....
7958.               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=1070095&projectid=70085&pathid=1049
Status	New

The zonemd_lookup_dnskey method calls the snprintf function, at line 8350 of ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	8387	8387
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/authzone.c
Method	zonemd_lookup_dnskey(struct auth_zone* z, struct module_env* env)

```
....
8387.           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=1070095&projectid=70085&pathid=1050
Status	New

The channel_post_x11_listener method calls the snprintf function, at line 1774 of ravynos-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	ravynos-1/channels.c	ravynos-1/channels.c
Line	1806	1806
Object	snprintf	snprintf

Code Snippet

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

```
....
1806.       snprintf(buf, sizeof buf, "X11 connection from %.200s port
%d",
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1051
Status	New

The channel_setup_fwd_listener_tcpip method calls the snprintf function, at line 3721 of ravynos-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	ravynos-1/channels.c	ravynos-1/channels.c
Line	3763	3763
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3763.        snprintf(strport, sizeof strport, "%d", fwd->listen_port);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1052
Status	New

The connect_to_helper method calls the snprintf function, at line 4598 of ravynos-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	ravynos-1/channels.c	ravynos-1/channels.c
Line	4636	4636
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/channels.c
Method connect_to_helper(struct ssh *ssh, const char *name, int port, int socktype,

```
....
4636.            snprintf(strport, sizeof strport, "%d", port);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1053
Status	New

The x11_create_display_inet method calls the snprintf function, at line 4939 of ravynos-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	ravynos-1/channels.c	ravynos-1/channels.c
Line	4961	4961
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/channels.c
Method x11_create_display_inet(struct ssh *ssh, int x11_display_offset,

```
....
4961.               snprintf(strport, sizeof strport, "%d", port);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1054
Status	New

The connect_local_xsocket method calls the snprintf function, at line 5061 of ravynos-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	ravynos-1/channels.c	ravynos-1/channels.c
Line	5064	5064
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/channels.c
Method connect_local_xsocket(u_int dnr)

```
....
5064.         snprintf(buf, sizeof buf, _PATH_UNIX_X, dnr);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1055
Status	New

The x11_connect_display method calls the snprintf function, at line 5096 of ravynos-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	ravynos-1/channels.c	ravynos-1/channels.c
Line	5180	5180
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/channels.c
Method	x11_connect_display(struct ssh *ssh)

```
....
5180.        snprintf(strport, sizeof strport, "%u", 6000 +
display_number);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1056
Status	New

The real_doit method calls the snprintf function, at line 140 of ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	148	148
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	real_doit(unsigned long cmd, void *data, const char *cmdstr)

```
....
148.              snprintf(buf, sizeof(buf), "/dev/%s", nexus);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1057
Status	New

The display_clip method calls the snprintf function, at line 3488 of ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3500	3500
Object	snprintf	snprintf

Code Snippet

File Name ravynos-1/cxgbetool.c
Method display_clip(void)

```
....
3500.         snprintf(name, sizeof(name), "dev.t%unex.%u.misc.clip",
chip_id, inst);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1058
Status	New

The doit method calls the snprintf function, at line 128 of ravynos-1/cxgbtool.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	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	134	134
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/cxgbtool.c
Method doit(const char *iff_name, unsigned long cmd, void *data)

```
....
134.              snprintf(buf, 64, "/dev/%s", iff_name);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1059
Status	New

The show_filters method calls the sprintf function, at line 1284 of ravynos-1/cxgbtool.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	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1314	1314
Object	sprintf	sprintf

Code Snippet
File Name ravynos-1/cxgbtool.c

Method	show_filters(const char *iff_name)

```
....
1314.                sprintf(sip, "%u.%u.%u.%u/%-2u", nsip.octet[0],
nsip.octet[1],
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1060
Status	New

The show_filters method calls the sprintf function, at line 1284 of ravynos-1/cxgbtool.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	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1317	1317
Object	sprintf	sprintf

Code Snippet

File Name	ravynos-1/cxgbtool.c
Method	show_filters(const char *iff_name)

```
....
1317.                sprintf(dip, "%u.%u.%u.%u", ndip.octet[0],
ndip.octet[1],
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1061
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	208	208
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
208.                snprintf(tmpfile, sizeof(tmpfile),
"/tmp/gvinum.XXXXXX");
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1062
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	225	225
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
225.                snprintf(commandline, sizeof(commandline), "%s %s",
ed,
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1063
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	293	293
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
293.                    snprintf(buf1, sizeof(buf1), "volume%d",
volumes);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1064
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	313	313
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
313.                        snprintf(p->name, sizeof(p->name),
"%s.p%d",
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1065
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	319	319
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
319.                                snprintf(p->volume, sizeof(p->volume),
"%s",
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1066
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	329	329
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
329.                          snprintf(buf1, sizeof(buf1), "plex%d", plexes);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1067
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	350	350
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
350.                                    snprintf(s->name, sizeof(s->name),
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1068
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	354	354
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
354.                                    snprintf(s->name, sizeof(s->name),
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1069
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	361	361
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
361.                            snprintf(s->plex, sizeof(s->plex), "%s", 
plex);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1070
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	363	363
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
363.                        snprintf(buf1, sizeof(buf1), "sd%d", subdisks);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1071
Status	New

The gvinum_create method calls the snprintf function, at line 175 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	379	379
Object	snprintf	snprintf

Code Snippet	
File Name	ravynos-1/gvinum.c
Method	gvinum_create(int argc, char * const *argv)

```
....
379.                    snprintf(buf1, sizeof(buf1), "drive%d", drives);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1072
Status	New

The create_volume method calls the snprintf function, at line 489 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	520	520
Object	snprintf	snprintf

Code Snippet	
File Name	ravynos-1/gvinum.c
Method	create_volume(int argc, char * const *argv, const char *verb)

```
....
520.                    snprintf(buf, sizeof(buf), "drive%d", drives++);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1073
Status	New

The find_name method calls the snprintf function, at line 569 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	601	601
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	find_name(const char *prefix, int type, int namelen)

```
....
601.              snprintf(sname, namelen, "%s%d", prefix, n);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1074
Status	New

The gvinum_list method calls the snprintf function, at line 806 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	858	858
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_list(int argc, char * const *argv)

```
....
858.                    snprintf(buf, sizeof(buf), "argv%d", i);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1075
Status	New

The gvinum_move method calls the snprintf function, at line 887 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	930	930
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c

Method	gvinum_move(int argc, char * const *argv)

```
....
930.                    snprintf(buf, sizeof(buf), "argv%d", i);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1076
Status	New

The gvinum_rm method calls the snprintf function, at line 1061 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1093	1093
Object	snprintf	snprintf

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_rm(int argc, char * const *argv)

```
....
1093.                       snprintf(buf, sizeof(buf), "argv%d", i);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1077
Status	New

The gvinum_resetconfig method calls the fgets function, at line 1107 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1136	1136
Object	fgets	fgets

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_resetconfig(int argc, char * const *argv)

```
....
1136.                fgets(reply, sizeof(reply), stdin);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1078
Status	New

The gvinum_start method calls the snprintf function, at line 1171 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1208	1208
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_start(int argc, char * const *argv)

```
....
1208.                       snprintf(buf, sizeof(buf), "argv%d", i);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1079
Status	New

The gvinum_grow method calls the snprintf function, at line 1270 of ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1312	1312
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_grow(int argc, char * const *argv)

```
....
1312.       snprintf(sdprefix, sizeof(sdprefix), "%s.s", argv[1]);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1080
Status	New

The http_digest_auth method calls the sprintf function, at line 1249 of ravynos-1/http.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	ravynos-1/http.c	ravynos-1/http.c
Line	1275	1275
Object	sprintf	sprintf

Code Snippet
File Name ravynos-1/http.c
Method http_digest_auth(conn_t *conn, const char *hdr, http_auth_challenge_t *c,

```
....
1275.           sprintf(noncecount, "%08x", c->nc);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1081
Status	New

The http_digest_auth method calls the sprintf function, at line 1249 of ravynos-1/http.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	ravynos-1/http.c	ravynos-1/http.c
Line	1277	1277
Object	sprintf	sprintf

Code Snippet
File Name ravynos-1/http.c
Method http_digest_auth(conn_t *conn, const char *hdr, http_auth_challenge_t *c,

```
....
1277.            sprintf(cnonce, "%x%lx", getpid(), (unsigned
long)time(0));
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1082
Status	New

The http_request_body method calls the snprintf function, at line 1585 of ravynos-1/http.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	ravynos-1/http.c	ravynos-1/http.c
Line	1656	1656
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1656.                    snprintf(hbuf, sizeof(hbuf), "%s:%d", host, url-
>port);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1083
Status	New

The bge_probe method calls the snprintf function, at line 2702 of ravynos-1/if_bge.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	ravynos-1/if_bge.c	ravynos-1/if_bge.c
Line	2724	2724
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/if_bge.c

Method bge_probe(device_t dev)

```
....
2724.                           snprintf(model, sizeof(model), "%s",
pname);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1084
Status	New

The bge_probe method calls the snprintf function, at line 2702 of ravynos-1/if_bge.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	ravynos-1/if_bge.c	ravynos-1/if_bge.c
Line	2727	2727
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/if_bge.c
Method bge_probe(device_t dev)

```
....
2727.                           snprintf(model, sizeof(model), "%s %s",
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1085
Status	New

The bge_probe method calls the snprintf function, at line 2702 of ravynos-1/if_bge.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	ravynos-1/if_bge.c	ravynos-1/if_bge.c
Line	2732	2732
Object	snprintf	snprintf

Code Snippet
File Name ravynos-1/if_bge.c

Method	bge_probe(device_t dev)

```
....
2732.                          snprintf(buf, sizeof(buf), "%s, %sASIC rev.
%#08x",
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1086
Status	New

The predicate_add method calls the sprintf function, at line 590 of ravynos-1/lockstat.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	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	609	609
Object	sprintf	sprintf

Code Snippet	
File Name	ravynos-1/lockstat.c
Method	predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
609.                          (void) sprintf(new, "(%s) && (%s %s %p)",
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1087
Status	New

The predicate_add method calls the sprintf function, at line 590 of ravynos-1/lockstat.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	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	612	612
Object	sprintf	sprintf

Code Snippet	
File Name	ravynos-1/lockstat.c

Method predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
612.                    (void) sprintf(new, "(%s) && (%s)", *pred,
what);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1088
Status	New

The predicate_add method calls the sprintf function, at line 590 of ravynos-1/lockstat.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	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	616	616
Object	sprintf	sprintf

Code Snippet
File Name ravynos-1/lockstat.c
Method predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
616.                    (void) sprintf(new, "%s %s %p",
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1089
Status	New

The predicate_add method calls the sprintf function, at line 590 of ravynos-1/lockstat.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	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	619	619
Object	sprintf	sprintf

Code Snippet
File Name ravynos-1/lockstat.c

Method predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
619.                    (void) sprintf(new, "%s", what);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1090
Status	New

The filter_add method calls the sprintf function, at line 635 of ravynos-1/lockstat.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	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	646	646
Object	sprintf	sprintf

Code Snippet
File Name ravynos-1/lockstat.c
Method filter_add(char **filt, char *what, uintptr_t base, size_t size)

```
....
646.            (void) sprintf(c, "%s(%s >= 0x%p && %s < 0x%p)", *filt[0] !=
'\0' ?
```

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=1070095&projectid=70085&pathid=1800
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1586	1586

Object	j	j

Code Snippet

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	parse_digest(struct archive_read *a, struct archive_entry *entry,

```
....
1586.                digest_buf[j] = high << 4 | low;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1801
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	2737	2737
Object	rrset_count	rrset_count

Code Snippet

File Name	ravynos-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=1070095&projectid=70085&pathid=1802
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	279	279
Object	i	i

Code Snippet

File Name	ravynos-1/buf.c
Method	translit_text(char *s, int len, int from, int to)

```
....
279.        ctab[i] = i;                  /* restore table to initial
state */
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1803
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	482	482
Object	found	found

Code Snippet

File Name	ravynos-1/channels.c
Method	channel_new(struct ssh *ssh, char *ctype, int type, int rfd, int wfd, int efd,

```
....
482.        c = sc->channels[found] = xcalloc(1, sizeof(Channel));
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1804
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2492	2492
Object	SSH_CHANNEL_X11_LISTENER	SSH_CHANNEL_X11_LISTENER

Code Snippet

File Name	ravynos-1/channels.c
Method	channel_handler_init(struct ssh_channels *sc)

```
....
2492.       pre[SSH_CHANNEL_X11_LISTENER] =
      &channel_pre_listener;
```

Unchecked Array Index\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1805
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2493	2493
Object	SSH_CHANNEL_AUTH_SOCKET	SSH_CHANNEL_AUTH_SOCKET

Code Snippet
File Name ravynos-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2493.        pre[SSH_CHANNEL_AUTH_SOCKET] =
      &channel_pre_listener;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1806
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2494	2494
Object	SSH_CHANNEL_CONNECTING	SSH_CHANNEL_CONNECTING

Code Snippet
File Name ravynos-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2494.        pre[SSH_CHANNEL_CONNECTING] =        &channel_pre_connecting;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1807
Status	New

	Source	Destination

File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2505	2505
Object	SSH_CHANNEL_X11_LISTENER	SSH_CHANNEL_X11_LISTENER

Code Snippet
File Name ravynos-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2505.        post[SSH_CHANNEL_X11_LISTENER] =
       &channel_post_x11_listener;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1808
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2506	2506
Object	SSH_CHANNEL_AUTH_SOCKET	SSH_CHANNEL_AUTH_SOCKET

Code Snippet
File Name ravynos-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2506.        post[SSH_CHANNEL_AUTH_SOCKET] =
       &channel_post_auth_listener;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1809
Status	New

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	2507	2507
Object	SSH_CHANNEL_CONNECTING	SSH_CHANNEL_CONNECTING

Code Snippet

File Name ravynos-1/channels.c
Method channel_handler_init(struct ssh_channels *sc)

```
....
2507.         post[SSH_CHANNEL_CONNECTING] =
       &channel_post_connecting;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1810
Status	New

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	2867	2867
Object	ru_alloc	ru_alloc

Code Snippet
File Name ravynos-1/dp_rx.c
Method static void ath11k_dp_rx_update_peer_stats(struct ath11k_sta *arsta,

```
....
2867.         rx_stats->ru_alloc_cnt[ppdu_info->ru_alloc] += num_msdu;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1811
Status	New

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	736	736
Object	l	l

Code Snippet
File Name ravynos-1/http.c
Method http_header_lex(const char **cpp, char *buf)

```
....
736.         buf[l] = 0;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1812
Status	New

	Source	Destination
File	ravynos-1/if_bge.c	ravynos-1/if_bge.c
Line	5314	5314
Object	idx	idx

Code Snippet
File Name ravynos-1/if_bge.c
Method bge_encap(struct bge_softc *sc, struct mbuf **m_head, uint32_t *txidx)

```
....
5314.         sc->bge_cdata.bge_tx_dmamap[idx] = map;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1813
Status	New

	Source	Destination
File	ravynos-1/if_bge.c	ravynos-1/if_bge.c
Line	5315	5315
Object	idx	idx

Code Snippet
File Name ravynos-1/if_bge.c
Method bge_encap(struct bge_softc *sc, struct mbuf **m_head, uint32_t *txidx)

```
....
5315.         sc->bge_cdata.bge_tx_chain[idx] = m;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1814
Status	New

	Source	Destination

File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	78	78
Object	id	id

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_init(struct module_env* env, int id)

```
....
78.    env->modinfo[id] = (void*)ipsecmod_env;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1815
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	106	106
Object	id	id

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_new(struct module_qstate* qstate, int id)

```
....
106.        qstate->minfo[id] = iq;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1816
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	126	126
Object	id	id

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_error(struct module_qstate* qstate, int id)

```
....
126.        qstate->ext_state[id] = module_error;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1817
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	171	171
Object	id	id

Code Snippet
File Name ravynos-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1818
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	394	394
Object	id	id

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_handle_query(struct module_qstate* qstate,

```
....
394.                qstate->ext_state[id] = module_wait_module;
```

Unchecked Array Index\Path 20:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1819
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	410	410
Object	id	id

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_handle_query(struct module_qstate* qstate,

```
....
410.                qstate->ext_state[id] = module_wait_module;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1820
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	462	462
Object	id	id

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_handle_query(struct module_qstate* qstate,

```
....
462.          qstate->ext_state[id] = module_finished;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1821
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	601	601

Object	id	id

Code Snippet
File Name ravynos-1/ipsecmod.c
Method ipsecmod_clear(struct module_qstate* qstate, int id)

```
....
601.        qstate->minfo[id] = NULL;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1822
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	468	468
Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
468.        s[IPOPT_OPTVAL] = IPOPT_NOP;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1823
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	475	475
Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
475.                s[IPOPT_OPTVAL] = IPOPT_TS;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1824
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	476	476
Object	IPOPT_OLEN	IPOPT_OLEN

Code Snippet
File Name	ravynos-1/iptests.c
Method	void	ip_test2(dev, mtu, ip, gwip, ptest)

```
....
476.                s[IPOPT_OLEN] = 4;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1825
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	477	477
Object	IPOPT_OFFSET	IPOPT_OFFSET

Code Snippet
File Name	ravynos-1/iptests.c
Method	void	ip_test2(dev, mtu, ip, gwip, ptest)

```
....
477.                s[IPOPT_OFFSET] = IPOPT_MINOFF;
```

Unchecked Array Index\Path 27:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1826
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	492	492
Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
492.                 s[IPOPT_OPTVAL] = IPOPT_RR;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1827
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	493	493
Object	IPOPT_OLEN	IPOPT_OLEN

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
493.                 s[IPOPT_OLEN] = 0;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1828
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	499	499

Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
499.                 s[IPOPT_OPTVAL] = IPOPT_TS;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1829
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	500	500
Object	IPOPT_OLEN	IPOPT_OLEN

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
500.                 s[IPOPT_OLEN] = 0;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1830
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	506	506
Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
506.                s[IPOPT_OPTVAL] = IPOPT_SECURITY;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1831
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	507	507
Object	IPOPT_OLEN	IPOPT_OLEN

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
507.                s[IPOPT_OLEN] = 0;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1832
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	513	513
Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
513.                s[IPOPT_OPTVAL] = IPOPT_LSRR;
```

Unchecked Array Index\Path 34:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1833
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	514	514
Object	IPOPT_OLEN	IPOPT_OLEN

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
514.                s[IPOPT_OLEN] = 0;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1834
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	520	520
Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
520.                s[IPOPT_OPTVAL] = IPOPT_SATID;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1835
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	521	521

Object	IPOPT_OLEN	IPOPT_OLEN

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
521.                    s[IPOPT_OLEN] = 0;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1836
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	527	527
Object	IPOPT_OPTVAL	IPOPT_OPTVAL

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
527.                    s[IPOPT_OPTVAL] = IPOPT_SSRR;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1837
Status	New

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	528	528
Object	IPOPT_OLEN	IPOPT_OLEN

Code Snippet
File Name ravynos-1/iptests.c
Method void ip_test2(dev, mtu, ip, gwip, ptest)

```
....
528.                s[IPOPT_OLEN] = 0;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1838
Status	New

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1033	1033
Object	j	j

Code Snippet
File Name ravynos-1/lockstat.c
Method process_aggregate(const dtrace_aggdata_t *agg, void *arg)

```
....
1033.                       lsrec->ls_hist[j] = quantized[i];
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1839
Status	New

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	4737	4737
Object	ids	ids

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_get_ld_list(struct mrsas_softc *sc)

```
....
4737.                             sc->ld_ids[ids] = ld_list_mem-
>ldList[ld_index].ref.ld_context.targetId;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1840
Status	New

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	252	252
Object	k	k

Code Snippet

File Name ravynos-1/name.c

Method _hx509_Name_to_string(const Name *n, char **str)

```
....
252.            ss[k] = '\0';
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1841
Status	New

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	277	277
Object	k	k

Code Snippet

File Name ravynos-1/name.c

Method _hx509_Name_to_string(const Name *n, char **str)

```
....
277.            ss[k] = '\0';
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1842
Status	New

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c

Line	644	644
Object	pstr_len	pstr_len

Code Snippet

File Name	ravynos-1/name.c
Method	hx509_parse_name(hx509_context context, const char *str, hx509_name *name)

```
....
644.            r[pstr_len] = '\0';
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1843
Status	New

	Source	Destination
File	ravynos-1/o_str.c	ravynos-1/o_str.c
Line	52	52
Object	maxlen	maxlen

Code Snippet

File Name	ravynos-1/o_str.c
Method	char *CRYPTO_strndup(const char *str, size_t s, const char* file, int line)

```
....
52.         ret[maxlen] = '\0';
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1844
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2166	2166
Object	pos	pos

Code Snippet

File Name	ravynos-1/pmcstudy.c
Method	read_a_line(FILE *io)

```
....
2166.              cnts[i].vals[pos] = strtol(p, &stop, 0);
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1845
Status	New

	Source	Destination
File	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	621	621
Object	CHET_ST	CHET_ST

Code Snippet

File Name	ravynos-1/scsi_ch.c
Method	chdone(struct cam_periph *periph, union ccb *done_ccb)

```
....
621.                    softc->sc_firsts[CHET_ST] = scsi_2btoul(ea-
>fsea);
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1846
Status	New

	Source	Destination
File	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	622	622
Object	CHET_ST	CHET_ST

Code Snippet

File Name	ravynos-1/scsi_ch.c
Method	chdone(struct cam_periph *periph, union ccb *done_ccb)

```
....
622.                    softc->sc_counts[CHET_ST] = scsi_2btoul(ea-
>nse);
```

Unchecked Array Index\Path 48:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1847
Status	New

	Source	Destination
File	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	623	623
Object	CHET_IE	CHET_IE

Code Snippet

File Name ravynos-1/scsi_ch.c

Method chdone(struct cam_periph *periph, union ccb *done_ccb)

```
....
623.                        softc->sc_firsts[CHET_IE] = scsi_2btoul(ea-
>fieea);
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1848
Status	New

	Source	Destination
File	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	624	624
Object	CHET_IE	CHET_IE

Code Snippet

File Name ravynos-1/scsi_ch.c

Method chdone(struct cam_periph *periph, union ccb *done_ccb)

```
....
624.                        softc->sc_counts[CHET_IE] = scsi_2btoul(ea-
>niee);
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1849
Status	New

	Source	Destination

File	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	1621	1621
Object	CHET_ST	CHET_ST

Code Snippet
File Name ravynos-1/scsi_ch.c
Method chgetparams(struct cam_periph *periph)

```
....
1621.       softc->sc_firsts[CHET_ST] = scsi_2btoul(ea->fsea);
```

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=1070095&projectid=70085&pathid=1765
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_lha.c	ravynos-1/archive_read_support_format_lha.c
Line	482	504
Object	signature	sizeof

Code Snippet
File Name ravynos-1/archive_read_support_format_lha.c
Method archive_read_format_lha_read_header(struct archive_read *a,

```
....
482.        const char *signature;
....
504.                signature = __archive_read_ahead(a,
sizeof(signature[0]), NULL);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1766
Status	New

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c

Line	72	73
Object	ipsecmod_env	sizeof

Code Snippet

File Name	ravynos-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 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1767
Status	New

	Source	Destination
File	ravynos-1/name.c	ravynos-1/name.c
Line	337	369
Object	name	sizeof

Code Snippet

File Name	ravynos-1/name.c
Method	dsstringprep(const DirectoryString *ds, uint32_t **rname, size_t *rlen)

```
....
337.      uint32_t *name;
....
369.        name = malloc(len * sizeof(name[0]));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1768
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	625
Object	lspping_tlv_header	sizeof

Code Snippet

File Name	ravynos-1/print-lspping.c
Method	lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
625.              tptr+=sizeof(struct lspping_tlv_header);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1769
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	609
Object	lspping_tlv_header	sizeof

Code Snippet

File Name	ravynos-1/print-lspping.c
Method	lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
609.          if (tlen < sizeof(struct lspping_tlv_header))
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1770
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	626
Object	lspping_tlv_header	sizeof

Code Snippet

File Name	ravynos-1/print-lspping.c
Method	lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
626.              tlen-=sizeof(struct lspping_tlv_header);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1771
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	630
Object	lspping_tlv_header	sizeof

Code Snippet

File Name	ravynos-1/print-lspping.c
Method	lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
630.          tlv_tptr=tptr+sizeof(struct lspping_tlv_header);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1772
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	634
Object	lspping_tlv_header	sizeof

Code Snippet

File Name	ravynos-1/print-lspping.c
Method	lspping_print(netdissect_options *ndo,

```
....
494.        const struct lspping_tlv_header *lspping_tlv_header;
....
634.            if (tlen < lspping_tlv_len+sizeof(struct
lspping_tlv_header))
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1773
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	644
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.        const struct lspping_tlv_header *lspping_tlv_header;
....
644.                    if (tlv_tlen < sizeof(struct lspping_tlv_header))
{
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1774
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	654
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.        const struct lspping_tlv_header *lspping_tlv_header;
....
654.                    subtlv_tptr=tlv_tptr+sizeof(struct 
lspping_tlv_header);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1775
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	657
Object	lspping_tlv_header	sizeof

Code Snippet

File Name	ravynos-1/print-lspping.c
Method	lspping_print(netdissect_options *ndo,

```
....
494.        const struct lspping_tlv_header *lspping_tlv_header;
....
657.                    if (tlv_tlen < lspping_subtlv_len+sizeof(struct 
lspping_tlv_header)) {
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1776
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	863
Object	lspping_tlv_header	sizeof

Code Snippet

File Name	ravynos-1/print-lspping.c
Method	lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
863.                      print_unknown_data(ndo, tlv_tptr+sizeof(struct
lspping_tlv_header),
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1777
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	871
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
871.                      if (tlv_tlen <
lspping_subtlv_len+sizeof(struct lspping_tlv_header)) {
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1778
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	877
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
877.                  tlv_tlen-=lspping_subtlv_len+sizeof(struct
lspping_tlv_header);
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1779
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	1059
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
1059.              print_unknown_data(ndo, tptr+sizeof(struct
lspping_tlv_header), "\n\t    ",
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1780
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	1067
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
1067.                 if (tlen < lspping_tlv_len+sizeof(struct
lspping_tlv_header))
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1781
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	1071
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.      const struct lspping_tlv_header *lspping_tlv_header;
....
1071.           tptr+=lspping_tlv_len+sizeof(struct lspping_tlv_header);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1782
Status	New

	Source	Destination
File	ravynos-1/print-lspping.c	ravynos-1/print-lspping.c
Line	494	1072
Object	lspping_tlv_header	sizeof

Code Snippet
File Name ravynos-1/print-lspping.c
Method lspping_print(netdissect_options *ndo,

```
....
494.       const struct lspping_tlv_header *lspping_tlv_header;
....
1072.          tlen-=lspping_tlv_len+sizeof(struct lspping_tlv_header);
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1783
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	147	147
Object	sizeof	sizeof

Code Snippet
File Name ravynos-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1784
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	153	153
Object	sizeof	sizeof

Code Snippet
File Name ravynos-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 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1785
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	157	157
Object	sizeof	sizeof

Code Snippet
File Name ravynos-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 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1786
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	740	740
Object	sizeof	sizeof

Code Snippet
File Name ravynos-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 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1787
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	802	802
Object	sizeof	sizeof

Code Snippet
File Name ravynos-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 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1788
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	881	881
Object	sizeof	sizeof

Code Snippet
File Name ravynos-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 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1789
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	955	955
Object	sizeof	sizeof

Code Snippet

File Name	ravynos-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 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1790
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1016	1016
Object	sizeof	sizeof

Code Snippet

File Name	ravynos-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 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1791
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1018	1018
Object	sizeof	sizeof

Code Snippet

File Name	ravynos-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 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1792
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	2697	2697
Object	sizeof	sizeof

Code Snippet
File Name ravynos-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 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1793
Status	New

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1609	1609
Object	sizeof	sizeof

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

```
....
1609.           sizeof (void *))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1794
Status	New

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	2846	2846
Object	sizeof	sizeof

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_alloc_mpt_cmds(struct mrsas_softc *sc)

```
....
2846.        sc->mpt_cmd_list = malloc(sizeof(struct mrsas_mpt_cmd *) *
max_fw_cmds,
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1795
Status	New

	Source	Destination
File	ravynos-1/mrsas.c	ravynos-1/mrsas.c
Line	2852	2852
Object	sizeof	sizeof

Code Snippet
File Name ravynos-1/mrsas.c
Method mrsas_alloc_mpt_cmds(struct mrsas_softc *sc)

```
....
2852.        memset(sc->mpt_cmd_list, 0, sizeof(struct mrsas_mpt_cmd *) *
max_fw_cmds);
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1796
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2501	2501
Object	sizeof	sizeof

Code Snippet	
File Name	ravynos-1/pmcstudy.c
Method	get_cpuid_set(void)

```
....
2501.                 sz = sizeof(char *) * pmc_allocated_cnt;
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1797
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2534	2534
Object	sizeof	sizeof

Code Snippet	
File Name	ravynos-1/pmcstudy.c
Method	get_cpuid_set(void)

```
....
2534.                       sz = sizeof(char *) * (pmc_allocated_cnt * 2);
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1798
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2697	2697
Object	sizeof	sizeof

Code Snippet	
File Name	ravynos-1/pmcstudy.c
Method	build_command_for_exp(struct expression *exp)

```
....
2697.         mal = cnt_pmc * sizeof(char *);
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1799
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	214	214
Object	sizeof	sizeof

Code Snippet
File Name ravynos-1/test_x509.c
Method HT_new(void)

```
....
214.        ht->buckets = xmalloc(ht->num_buckets * sizeof(ht_elt *));
```

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=1070095&projectid=70085&pathid=1368
Status	New

The size of the buffer used by ipseckey_has_safe_characters in "%d %d %d %s ", at line 215 of ravynos-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 ravynos-1/ipsecmod.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/ipsecmod.c	ravynos-1/ipsecmod.c
Line	223	223
Object	"%d %d %d %s "	"%d %d %d %s "

Code Snippet
File Name ravynos-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=1070095&projectid=70085&pathid=1369
Status	New

The size of the buffer used by predicate_add in "(%s) && (%s %s %p)", at line 590 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that predicate_add passes to "(%s) && (%s %s %p)", at line 590 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	609	609
Object	"(%s) && (%s %s %p)"	"(%s) && (%s %s %p)"

Code Snippet
File Name ravynos-1/lockstat.c
Method predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
609.                (void) sprintf(new, "(%s) && (%s %s %p)",
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1370
Status	New

The size of the buffer used by predicate_add in "(%s) && (%s)", at line 590 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that predicate_add passes to "(%s) && (%s)", at line 590 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	612	612
Object	"(%s) && (%s)"	"(%s) && (%s)"

Code Snippet
File Name ravynos-1/lockstat.c
Method predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
612.                    (void) sprintf(new, "(%s) && (%s)", *pred,
what);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1371
Status	New

The size of the buffer used by predicate_add in "%s %s %p", at line 590 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that predicate_add passes to "%s %s %p", at line 590 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	616	616
Object	"%s %s %p"	"%s %s %p"

Code Snippet

File Name	ravynos-1/lockstat.c
Method	predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
616.                    (void) sprintf(new, "%s %s %p",
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1372
Status	New

The size of the buffer used by predicate_add in "%s", at line 590 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that predicate_add passes to "%s", at line 590 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	619	619
Object	"%s"	"%s"

Code Snippet

File Name	ravynos-1/lockstat.c
Method	predicate_add(char **pred, char *what, char *cmp, uintptr_t value)

```
....
619.                    (void) sprintf(new, "%s", what);
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1373
Status	New

The size of the buffer used by filter_add in "%s(%s >= 0x%p && %s < 0x%p)", at line 635 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that filter_add passes to "%s(%s >= 0x%p && %s < 0x%p)", at line 635 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	646	646
Object	"%s(%s >= 0x%p && %s < 0x%p)"	"%s(%s >= 0x%p && %s < 0x%p)"

Code Snippet

File Name	ravynos-1/lockstat.c
Method	filter_add(char **filt, char *what, uintptr_t base, size_t size)

```
....
646.            (void) sprintf(c, "%s(%s >= 0x%p && %s < 0x%p)", *filt[0] !=
'\0' ?
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1374
Status	New

The size of the buffer used by format_symbol in "%s[%ld]", at line 1726 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that format_symbol passes to "%s[%ld]", at line 1726 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1735	1735
Object	"%s[%ld]"	"%s[%ld]"

Code Snippet

File Name	ravynos-1/lockstat.c
Method	format_symbol(char *buf, uintptr_t addr, int show_size)

```
....
1735.               (void) sprintf(buf, "%s[%ld]", symname,
(long)symsize);
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1375
Status	New

The size of the buffer used by format_symbol in "%s", at line 1726 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that format_symbol passes to "%s", at line 1726 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1737	1737
Object	"%s"	"%s"

Code Snippet
File Name ravynos-1/lockstat.c
Method format_symbol(char *buf, uintptr_t addr, int show_size)

```
....
1737.               (void) sprintf(buf, "%s", symname);
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1376
Status	New

The size of the buffer used by format_symbol in "%s+%ld", at line 1726 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that format_symbol passes to "%s+%ld", at line 1726 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1740	1740
Object	"%s+%ld"	"%s+%ld"

Code Snippet
File Name ravynos-1/lockstat.c
Method format_symbol(char *buf, uintptr_t addr, int show_size)

```
....
1740.             (void) sprintf(buf, "%s+%ld", symname, (long)symoff);
```

Potential Precision Problem\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1377
Status	New

The size of the buffer used by format_symbol in "%s+0x%llx", at line 1726 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that format_symbol passes to "%s+0x%llx", at line 1726 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1745	1745
Object	"%s+0x%llx"	"%s+0x%llx"

Code Snippet

File Name	ravynos-1/lockstat.c
Method	format_symbol(char *buf, uintptr_t addr, int show_size)

```
....
1745.             (void) sprintf(buf, "%s+0x%llx", symname,
```

Potential Precision Problem\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1378
Status	New

The size of the buffer used by report_stats in "%s%s", at line 1753 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that report_stats passes to "%s%s", at line 1753 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1777	1777
Object	"%s%s"	"%s%s"

Code Snippet

File Name	ravynos-1/lockstat.c
Method	report_stats(FILE *out, lsrec_t **sort_buf, size_t nrecs, uint64_t total_count,

```
....
1777.        (void) sprintf(lhdr, "%s%s",
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1379
Status	New

The size of the buffer used by report_stats in "%s%s", at line 1753 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that report_stats passes to "%s%s", at line 1753 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1779	1779
Object	"%s%s"	"%s%s"

Code Snippet
File Name ravynos-1/lockstat.c
Method report_stats(FILE *out, lsrec_t **sort_buf, size_t nrecs, uint64_t total_count,

```
....
1779.        (void) sprintf(chdr, "%s%s",
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1380
Status	New

The size of the buffer used by report_stats in "%s", at line 1753 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that report_stats passes to "%s", at line 1753 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1790	1790
Object	"%s"	"%s"

Code Snippet
File Name ravynos-1/lockstat.c
Method report_stats(FILE *out, lsrec_t **sort_buf, size_t nrecs, uint64_t total_count,

```
....
1790.              (void) sprintf(buf, "%s",
g_event_info[event].ev_units);
```

Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1381
Status	New

The size of the buffer used by report_stats in "%s", at line 1753 of ravynos-1/lockstat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that report_stats passes to "%s", at line 1753 of ravynos-1/lockstat.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1843	1843
Object	"%s"	"%s"

Code Snippet
File Name ravynos-1/lockstat.c
Method report_stats(FILE *out, lsrec_t **sort_buf, size_t nrecs, uint64_t total_count,

```
....
1843.                      (void) sprintf(buf, "%s",
```

Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1382
Status	New

The size of the buffer used by test_for_a_pmc in "/usr/sbin/pmcstat -w .25 -c 0 -s %s", at line 2568 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_for_a_pmc passes to "/usr/sbin/pmcstat -w .25 -c 0 -s %s", at line 2568 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2583	2583
Object	"/usr/sbin/pmcstat -w .25 -c 0 -s %s"	"/usr/sbin/pmcstat -w .25 -c 0 -s %s"

Code Snippet
File Name ravynos-1/pmcstudy.c
Method test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2583.       sprintf(my_command, "/usr/sbin/pmcstat -w .25 -c 0 -s %s",
pmc);
```

Potential Precision Problem\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1383
Status	New

The size of the buffer used by test_for_a_pmc in "%s", at line 2568 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_for_a_pmc passes to "%s", at line 2568 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2590	2590
Object	"%s"	"%s"

Code Snippet	
File Name	ravynos-1/pmcstudy.c
Method	test_for_a_pmc(const char *pmc, int out_so_far)

```
....
2590.       len = sprintf(resp, "%s", pmc);
```

Potential Precision Problem\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1384
Status	New

The size of the buffer used by build_command_for_exp in " -s %s", at line 2669 of ravynos-1/pmcstudy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that build_command_for_exp passes to " -s %s", at line 2669 of ravynos-1/pmcstudy.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2727	2727
Object	" -s %s"	" -s %s"

Code Snippet	
File Name	ravynos-1/pmcstudy.c
Method	build_command_for_exp(struct expression *exp)

```
....
2727.            sprintf(forming, " -s %s", vars[i]);
```

Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1385
Status	New

The size of the buffer used by action_disable in "%s:disable=", at line 308 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_disable passes to "%s:disable=", at line 308 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	320	320
Object	"%s:disable="	"%s:disable="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_disable(int argc, char **argv)

```
....
320.            sprintf(argv_disable, "%s:disable=", argv[i]);
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1386
Status	New

The size of the buffer used by action_enable in "%s:enable=", at line 329 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_enable passes to "%s:enable=", at line 329 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	341	341
Object	"%s:enable="	"%s:enable="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_enable(int argc, char **argv)

```
....
341.                sprintf(argv_enable, "%s:enable=", argv[i]);
```

Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1387
Status	New

The size of the buffer used by action_reload in "%s:reload=", at line 350 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_reload passes to "%s:reload=", at line 350 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	364	364
Object	"%s:reload="	"%s:reload="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_reload(int argc, char **argv)

```
....
364.                sprintf(argv_reload, "%s:reload=", argv[i]);
```

Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1388
Status	New

The size of the buffer used by action_show in "invalid interface %s", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "invalid interface %s", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	460	460
Object	"invalid interface %s"	"invalid interface %s"

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_show(int argc, char **argv)

```
....
460.                          sprintf(errmsgbuf, "invalid interface %s",
```

Potential Precision Problem\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1389
Status	New

The size of the buffer used by action_show in "%s:ifi=", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "%s:ifi=", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	483	483
Object	"%s:ifi="	"%s:ifi="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_show(int argc, char **argv)

```
....
483.              sprintf(argv_ifi, "%s:ifi=", ifi->ifi_ifname);
```

Potential Precision Problem\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1390
Status	New

The size of the buffer used by action_show in "%s:rai=", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "%s:rai=", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	550	550
Object	"%s:rai="	"%s:rai="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_show(int argc, char **argv)

```
....
550.                sprintf(argv_rai, "%s:rai=", ifi->ifi_ifname);
```

Potential Precision Problem\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1391
Status	New

The size of the buffer used by action_show in "%s:ifi_ra_timer=", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "%s:ifi_ra_timer=", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	601	601
Object	"%s:ifi_ra_timer="	"%s:ifi_ra_timer="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_show(int argc, char **argv)

```
....
601.                      sprintf(argv_ifi_ra_timer, "%s:ifi_ra_timer=",
```

Potential Precision Problem\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1392
Status	New

The size of the buffer used by action_show in "%s:rti=", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "%s:rti=", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	633	633
Object	"%s:rti="	"%s:rti="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_show(int argc, char **argv)

```
....
633.                    sprintf(argv_rti, "%s:rti=", ifi->ifi_ifname);
```

Potential Precision Problem\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1393
Status	New

The size of the buffer used by action_show in "%s:pfx=", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "%s:pfx=", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	649	649
Object	"%s:pfx="	"%s:pfx="

Code Snippet
File Name ravynos-1/rtadvctl.c
Method action_show(int argc, char **argv)

```
....
649.                    sprintf(argv_pfx, "%s:pfx=", ifi->ifi_ifname);
```

Potential Precision Problem\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1394
Status	New

The size of the buffer used by action_show in "%s:rdnss=", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "%s:rdnss=", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	667	667
Object	"%s:rdnss="	"%s:rdnss="

Code Snippet
File Name ravynos-1/rtadvctl.c
Method action_show(int argc, char **argv)

```
....
667.                sprintf(argv_rdnss, "%s:rdnss=", ifi->ifi_ifname);
```

Potential Precision Problem\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1395
Status	New

The size of the buffer used by action_show in "%s:dnssl=", at line 408 of ravynos-1/rtadvctl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that action_show passes to "%s:dnssl=", at line 408 of ravynos-1/rtadvctl.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	682	682
Object	"%s:dnssl="	"%s:dnssl="

Code Snippet

File Name	ravynos-1/rtadvctl.c
Method	action_show(int argc, char **argv)

```
....
682.                sprintf(argv_dnssl, "%s:dnssl=", ifi->ifi_ifname);
```

Potential Precision Problem\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1396
Status	New

The size of the buffer used by read_file in "%s/%s", at line 438 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_file passes to "%s/%s", at line 438 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	447	447
Object	"%s/%s"	"%s/%s"

Code Snippet

File Name	ravynos-1/test_x509.c
Method	read_file(const char *name, size_t *len)

```
....
447.        sprintf(dname, "%s/%s", DIRNAME, name);
```

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=1070095&projectid=70085&pathid=1409
Status	New

Method freebsd4_sendsig in ravynos-1/exec_machdep.c, at line 261, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	288	288
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/exec_machdep.c
Method freebsd4_sendsig(sig_t catcher, ksiginfo_t *ksi, sigset_t *mask)

```
....
288.        bcopy(regs, &sf.sf_uc.uc_mcontext.mc_fs, sizeof(*regs));
```

Use of Obsolete Functions\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1410
Status	New

Method sendsig in ravynos-1/exec_machdep.c, at line 380, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	431	431
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/exec_machdep.c
Method	sendsig(sig_t catcher, ksiginfo_t *ksi, sigset_t *mask)

```
....
431.        bcopy(regs, &sf.sf_uc.uc_mcontext.mc_fs, sizeof(*regs));
```

Use of Obsolete Functions\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1411
Status	New

Method freebsd4_sigreturn in ravynos-1/exec_machdep.c, at line 659, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	703	703
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/exec_machdep.c
Method	freebsd4_sigreturn(struct thread *td, struct freebsd4_sigreturn_args *uap)

```
....
703.            bcopy(&ucp->uc_mcontext.mc_fs, tf, sizeof(struct
trapframe));
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1412
Status	New

Method freebsd4_sigreturn in ravynos-1/exec_machdep.c, at line 659, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	741	741
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/exec_machdep.c
Method	freebsd4_sigreturn(struct thread *td, struct freebsd4_sigreturn_args *uap)

```
....
741.              bcopy(&ucp->uc_mcontext.mc_fs, regs, sizeof(*regs));
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1413
Status	New

Method sys_sigreturn in ravynos-1/exec_machdep.c, at line 757, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	812	812
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/exec_machdep.c
Method	sys_sigreturn(struct thread *td, struct sigreturn_args *uap)

```
....
812.              bcopy(&ucp->uc_mcontext.mc_fs, tf, sizeof(struct
trapframe));
```

Use of Obsolete Functions\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1414
Status	New

Method sys_sigreturn in ravynos-1/exec_machdep.c, at line 757, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	876	876
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/exec_machdep.c
Method	sys_sigreturn(struct thread *td, struct sigreturn_args *uap)

```
....
876.              bcopy(&ucp->uc_mcontext.mc_fs, regs, sizeof(*regs));
```

Use of Obsolete Functions\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1415
Status	New

Method fill_fpregs in ravynos-1/exec_machdep.c, at line 1076, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	1087	1087
Object	bcopy	bcopy

Code Snippet

File Name ravynos-1/exec_machdep.c

Method fill_fpregs(struct thread *td, struct fpreg *fpregs)

```
....
1087.              bcopy(&get_pcb_user_save_td(td)->sv_87, fpregs,
```

Use of Obsolete Functions\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1416
Status	New

Method set_fpregs in ravynos-1/exec_machdep.c, at line 1093, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	1101	1101
Object	bcopy	bcopy

Code Snippet

File Name ravynos-1/exec_machdep.c

Method set_fpregs(struct thread *td, struct fpreg *fpregs)

```
....
1101.              bcopy(fpregs, &get_pcb_user_save_td(td)->sv_87,
```

Use of Obsolete Functions\Path 9:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1417
Status	New

Method get_fpcontext in ravynos-1/exec_machdep.c, at line 1210, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	1216	1216
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/exec_machdep.c
Method	get_fpcontext(struct thread *td, mcontext_t *mcp, char *xfpusave,

```
....
1216.       bcopy(get_pcb_user_save_td(td), &mcp->mc_fpstate[0],
```

Use of Obsolete Functions\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1418
Status	New

Method get_fpcontext in ravynos-1/exec_machdep.c, at line 1210, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/exec_machdep.c	ravynos-1/exec_machdep.c
Line	1229	1229
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/exec_machdep.c
Method	get_fpcontext(struct thread *td, mcontext_t *mcp, char *xfpusave,

```
....
1229.       bcopy(get_pcb_user_save_td(td) + 1, xfpusave, len);
```

Use of Obsolete Functions\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1419
Status	New

Method bge_rxeof in ravynos-1/if_bge.c, at line 4302, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/if_bge.c	ravynos-1/if_bge.c
Line	4387	4387
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/if_bge.c
Method	bge_rxeof(struct bge_softc *sc, uint16_t rx_prod, int holdlck)

```
....
4387.                   bcopy(m->m_data, m->m_data + ETHER_ALIGN,
```

Use of Obsolete Functions\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1420
Status	New

Method ip_test7 in ravynos-1/iptests.c, at line 1322, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	1347	1347
Object	bcopy	bcopy

Code Snippet

File Name	ravynos-1/iptests.c
Method	ip_test7(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
1347.             bcopy((char *)&ip->ip_dst, (char *)&pip->ip_dst,
```

Use of Obsolete Functions\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1421
Status	New

Method ip_test7 in ravynos-1/iptests.c, at line 1322, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination

File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	1363	1363
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test7(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
1363.            bcopy((char *)&ip->ip_dst, (char *)&pip->ip_dst,
```

Use of Obsolete Functions\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1422
Status	New

Method ip_test5 in ravynos-1/iptests.c, at line 900, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	1082	1082
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test5(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
1082.        bcopy((char *)ip, (char *)&ti, sizeof(*ip));
```

Use of Obsolete Functions\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1423
Status	New

Method get_data in ravynos-1/krb5_mech.c, at line 158, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	167	167
Object	bcopy	bcopy

Code Snippet	
File Name	ravynos-1/krb5_mech.c
Method	get_data(const uint8_t **pp, size_t *lenp, struct krb5_data *dp)

```
....
167.         bcopy(*pp, dp->kd_data, sz);
```

Use of Obsolete Functions\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1424
Status	New

Method krb5_make_token in ravynos-1/krb5_mech.c, at line 557, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	614	614
Object	bcopy	bcopy

Code Snippet	
File Name	ravynos-1/krb5_mech.c
Method	krb5_make_token(char tok_id[2], size_t hlen, size_t len, struct mbuf **mp)

```
....
614.         bcopy(oid->elements, p, oid->length);
```

Use of Obsolete Functions\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1425
Status	New

Method krb5_get_mic_old in ravynos-1/krb5_mech.c, at line 860, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	898	898
Object	bcopy	bcopy

Code Snippet	
File Name	ravynos-1/krb5_mech.c
Method	krb5_get_mic_old(struct krb5_context *kc, struct mbuf *m,

```
....
898.        bcopy(tm->m_data, p + 8, cklen);
```

Use of Obsolete Functions\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1426
Status	New

Method krb5_get_mic_old in ravynos-1/krb5_mech.c, at line 860, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	933	933
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_get_mic_old(struct krb5_context *kc, struct mbuf *m,

```
....
933.        bcopy(p + 8, buf, 8);
```

Use of Obsolete Functions\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1427
Status	New

Method krb5_verify_mic_old in ravynos-1/krb5_mech.c, at line 1043, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1109	1109
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_verify_mic_old(struct krb5_context *kc, struct mbuf *m, struct mbuf *mic,

```
....
1109.       bcopy(p, tm->m_data, 8);
```

Use of Obsolete Functions\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1428
Status	New

Method krb5_wrap_old in ravynos-1/krb5_mech.c, at line 1251, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1336	1336
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_wrap_old(struct krb5_context *kc, int conf_req_flag,

```
....
1336.        bcopy(cm->m_data, p + 8, cklen);
```

Use of Obsolete Functions\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1429
Status	New

Method krb5_wrap_new in ravynos-1/krb5_mech.c, at line 1399, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1529	1529
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_wrap_new(struct krb5_context *kc, int conf_req_flag,

```
....
1529.              bcopy(p, tm->m_data, 16);
```

Use of Obsolete Functions\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=1430
Status	New

Method krb5_unwrap_new in ravynos-1/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1867	1867
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state)

```
....
1867.                    bcopy(m->m_data, buf, RRC);
```

Use of Obsolete Functions\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1431
Status	New

Method krb5_unwrap_new in ravynos-1/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1868	1868
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state)

```
....
1868.                    bcopy(m->m_data + RRC, m->m_data, rlen - RRC);
```

Use of Obsolete Functions\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1432
Status	New

Method krb5_unwrap_new in ravynos-1/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1869	1869
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state)

```
....
1869.                   bcopy(buf, m->m_data + rlen - RRC, RRC);
```

Use of Obsolete Functions\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1433
Status	New

Method krb5_unwrap_new in ravynos-1/krb5_mech.c, at line 1777, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/krb5_mech.c	ravynos-1/krb5_mech.c
Line	1955	1955
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/krb5_mech.c
Method krb5_unwrap_new(struct krb5_context *kc, struct mbuf **mp, int *conf_state)

```
....
1955.             bcopy(cm->m_data, buf, cklen);
```

Use of Obsolete Functions\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1434
Status	New

Method filter_add in ravynos-1/lockstat.c, at line 635, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	655	655

Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/lockstat.c
Method filter_add(char **filt, char *what, uintptr_t base, size_t size)

```
....
655.        bcopy(*filt, new, len);
```

Use of Obsolete Functions\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1435
Status	New

Method main in ravynos-1/lockstat.c, at line 1114, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1583	1583
Object	bcopy	bcopy

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

```
....
1583.                       bcopy(oldlsp, lsp, LS_TIME);
```

Use of Obsolete Functions\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1436
Status	New

Method main in ravynos-1/lockstat.c, at line 1114, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1592	1592
Object	bcopy	bcopy

Code Snippet
File Name ravynos-1/lockstat.c

Method	main(int argc, char **argv)

```
....
1592.                            bcopy(oldlsp, lsp, LS_TIME);
```

Use of Obsolete Functions\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1437
Status	New

Method copy_element_status in ravynos-1/scsi_ch.c, at line 1049, calls an obsolete API, bcopy. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	ravynos-1/scsi_ch.c	ravynos-1/scsi_ch.c
Line	1131	1131
Object	bcopy	bcopy

Code Snippet	
File Name	ravynos-1/scsi_ch.c
Method	copy_element_status(struct ch_softc *softc,

```
....
1131.                       bcopy((void *)devid->designator,
```

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=1070095&projectid=70085&pathid=1441
Status	New

	Source	Destination
File	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1563	1563
Object	digest_buf	sizeof

Code Snippet	
File Name	ravynos-1/archive_read_support_format_mtree.c
Method	parse_digest(struct archive_read *a, struct archive_entry *entry,

```
....
1563.          if (len > sizeof(digest_buf)) {
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1442
Status	New

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	177	177
Object	dtable	sizeof

Code Snippet
File Name ravynos-1/rtadvctl.c
Method main(int argc, char *argv[])

```
....
177.          for (i = 0; (size_t)i < sizeof(dtable)/sizeof(dtable[0]);
i++) {
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1443
Status	New

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c
Line	177	177
Object	dtable	sizeof

Code Snippet
File Name ravynos-1/rtadvctl.c
Method main(int argc, char *argv[])

```
....
177.          for (i = 0; (size_t)i < sizeof(dtable)/sizeof(dtable[0]);
i++) {
```

Sizeof Pointer Argument\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1444
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2651	2651
Object	string	sizeof

Code Snippet

File Name ravynos-1/cxgbetool.c

Method modinfo(int argc, const char *argv[])

```
....
2651.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1445
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2660	2660
Object	string	sizeof

Code Snippet

File Name ravynos-1/cxgbetool.c

Method modinfo(int argc, const char *argv[])

```
....
2660.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1446
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c

Line	2651	2660
Object	string	sizeof

Code Snippet
File Name ravynos-1/cxgbetool.c
Method modinfo(int argc, const char *argv[])

```
....
2651.       bzero(&string, sizeof(string));
....
2660.       bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1447
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2669	2669
Object	string	sizeof

Code Snippet
File Name ravynos-1/cxgbetool.c
Method modinfo(int argc, const char *argv[])

```
....
2669.       bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1448
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2660	2669
Object	string	sizeof

Code Snippet
File Name ravynos-1/cxgbetool.c
Method modinfo(int argc, const char *argv[])

```
....
2660.        bzero(&string, sizeof(string));
....
2669.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1449
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2651	2669
Object	string	sizeof

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	modinfo(int argc, const char *argv[])

```
....
2651.        bzero(&string, sizeof(string));
....
2669.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1450
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2678	2678
Object	string	sizeof

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	modinfo(int argc, const char *argv[])

```
....
2678.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1451
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2669	2678
Object	string	sizeof

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	modinfo(int argc, const char *argv[])

```
....
2669.        bzero(&string, sizeof(string));
....
2678.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1452
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2660	2678
Object	string	sizeof

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	modinfo(int argc, const char *argv[])

```
....
2660.        bzero(&string, sizeof(string));
....
2678.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1453

Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2651	2678
Object	string	sizeof

Code Snippet
File Name ravynos-1/cxgbetool.c
Method modinfo(int argc, const char *argv[])

```
....
2651.        bzero(&string, sizeof(string));
....
2678.        bzero(&string, sizeof(string));
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1454
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	854	854
Object	config	sizeof

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_list(int argc, char * const *argv)

```
....
854.        gctl_add_param(req, "config", sizeof(config), config,
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1455
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2813	2813

Object	glob_cpu	sizeof

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

```
....
2813.       memset(glob_cpu, 0, sizeof(glob_cpu));
```

Sizeof Pointer Argument\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1456
Status	New

	Source	Destination
File	ravynos-1/rec_layer_s3.c	ravynos-1/rec_layer_s3.c
Line	858	858
Object	wr	sizeof

Code Snippet
File Name ravynos-1/rec_layer_s3.c
Method int do_ssl3_write(SSL *s, int type, const unsigned char *buf,

```
....
858.       memset(wr, 0, sizeof(wr));
```

Sizeof Pointer Argument\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1457
Status	New

	Source	Destination
File	ravynos-1/snprintf.c	ravynos-1/snprintf.c
Line	1016	1016
Object	iconvert	sizeof

Code Snippet
File Name ravynos-1/snprintf.c
Method fmtint(char *str, size_t *len, size_t size, INTMAX_T value, int base, int width,

```
....
1016.        pos = convert(uvalue, iconvert, sizeof(iconvert), base,
```

Sizeof Pointer Argument\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1458
Status	New

	Source	Destination
File	ravynos-1/snprintf.c	ravynos-1/snprintf.c
Line	1289	1289
Object	iconvert	sizeof

Code Snippet
File Name ravynos-1/snprintf.c
Method fmtflt(char *str, size_t *len, size_t size, LDOUBLE fvalue, int width,

```
....
1289.        ipos = convert(intpart, iconvert, sizeof(iconvert), 10, 0);
```

Sizeof Pointer Argument\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1459
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1725	1725
Object	args	sizeof

Code Snippet
File Name ravynos-1/cxgbtool.c
Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1725.               for (i = 2; i < sizeof(args)/sizeof(args[0]) - 1; i++)
{
```

Sizeof Pointer Argument\Path 20:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1460
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1725	1725
Object	args	sizeof

Code Snippet
File Name ravynos-1/cxgbtool.c
Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1725.             for (i = 2; i < sizeof(args)/sizeof(args[0]) - 1; i++)
{
```

Sizeof Pointer Argument\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1461
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2946	2946
Object	glob_cpu	sizeof

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

```
....
2946.             memset(glob_cpu, 0, sizeof(glob_cpu));
```

Sizeof Pointer Argument\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1462
Status	New

	Source	Destination
File	ravynos-1/snprintf.c	ravynos-1/snprintf.c

Line	1291	1291
Object	fconvert	sizeof

Code Snippet
File Name ravynos-1/snprintf.c
Method fmtflt(char *str, size_t *len, size_t size, LDOUBLE fvalue, int width,

```
....
1291.             fpos = convert(fracpart, fconvert, sizeof(fconvert),
10, 0);
```

Sizeof Pointer Argument\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1463
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1090	1090
Object	tmp	sizeof

Code Snippet
File Name ravynos-1/test_x509.c
Method string_to_hash(const char *name)

```
....
1090.                   if (v == sizeof tmp) {
```

Sizeof Pointer Argument\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1464
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	1128	1128
Object	tmp	sizeof

Code Snippet
File Name ravynos-1/test_x509.c
Method string_to_curve(const char *name)

```
....
1128.                   if (v == sizeof tmp) {
```

Sizeof Pointer Argument\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1465
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1731	1731
Object	args	sizeof

Code Snippet

File Name ravynos-1/cxgbtool.c

Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1731.             args[sizeof(args)/sizeof(args[0]) - 1] = 0;
```

Sizeof Pointer Argument\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1466
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1725	1731
Object	args	sizeof

Code Snippet

File Name ravynos-1/cxgbtool.c

Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1725.             for (i = 2; i < sizeof(args)/sizeof(args[0]) - 1; i++)
{
....
1731.             args[sizeof(args)/sizeof(args[0]) - 1] = 0;
```

Sizeof Pointer Argument\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1467
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1725	1731
Object	args	sizeof

Code Snippet

File Name ravynos-1/cxgbtool.c

Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1725.             for (i = 2; i < sizeof(args)/sizeof(args[0]) - 1; i++)
{
....
1731.             args[sizeof(args)/sizeof(args[0]) - 1] = 0;
```

Sizeof Pointer Argument\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1468
Status	New

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1715	1715
Object	buf	sizeof

Code Snippet

File Name ravynos-1/cxgbtool.c

Method run_cmd_loop(int argc, char *argv[], const char *iff_name)

```
....
1715.             n = read(STDIN_FILENO, buf, sizeof(buf) - 1);
```

Sizeof Pointer Argument\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1469
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	327	327
Object	plex	sizeof

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
327.                    strlcpy(plex, p->name, sizeof(plex));
```

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=1070095&projectid=70085&pathid=1742
Status	New

The az_parse_file method in ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1516	1516
Object	fopen	fopen

Code Snippet
File Name ravynos-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=1070095&projectid=70085&pathid=1743
Status	New

The auth_zone_read_zonefile method in ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1585	1585
Object	fopen	fopen

Code Snippet

File Name	ravynos-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=1070095&projectid=70085&pathid=1744
Status	New

The auth_zone_write_file method in ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1733	1733
Object	fopen	fopen

Code Snippet

File Name	ravynos-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=1070095&projectid=70085&pathid=1745
Status	New

The auth_zone_write_chunks method in ravynos-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	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5147	5147
Object	fopen	fopen

Code Snippet
File Name ravynos-1/authzone.c
Method auth_zone_write_chunks(struct auth_xfer* xfr, const char* fname)

```
....
5147.        out = fopen(fname, "w");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1746
Status	New

The parse_offload_policy method in ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3386	3386
Object	fopen	fopen

Code Snippet
File Name ravynos-1/cxgbetool.c
Method parse_offload_policy(const char *fname, struct t4_offload_policy *op)

```
....
3386.        fp = fopen(fname, "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1747
Status	New

The gvinum_create method in ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	199	199
Object	fopen	fopen

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
199.                            if ((tmp = fopen(argv[i], "r")) == NULL) {
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1748
Status	New

The gvinum_create method in ravynos-1/gvinum.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	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	233	233
Object	fopen	fopen

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
233.                    if ((tmp = fopen(tmpfile, "r")) == NULL) {
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1749
Status	New

The main method in ravynos-1/lockstat.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	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1330	1330
Object	fopen	fopen

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

```
....
1330.                       if ((out = fopen(optarg, "w")) == NULL)
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1750
Status	New

The process_file method in ravynos-1/pmcstudy.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	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2257	2257
Object	fopen	fopen

Code Snippet
File Name ravynos-1/pmcstudy.c
Method process_file(char *filename)

```
....
2257.                io = fopen(filename, "r");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1751
Status	New

The load_server_config method in ravynos-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	ravynos-1/servconf.c	ravynos-1/servconf.c

Line	2628	2628
Object	fopen	fopen

Code Snippet
File Name ravynos-1/servconf.c
Method load_server_config(const char *filename, struct sshbuf *conf)

```
....
2628.        if ((f = fopen(filename, "r")) == NULL) {
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1752
Status	New

The read_file method in ravynos-1/test_x509.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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	450	450
Object	fopen	fopen

Code Snippet
File Name ravynos-1/test_x509.c
Method read_file(const char *name, size_t *len)

```
....
450.        f = fopen(name, "rb");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1753
Status	New

The conf_init method in ravynos-1/test_x509.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	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	612	612
Object	fopen	fopen

Code Snippet

File Name	ravynos-1/test_x509.c
Method	conf_init(const char *fname)

```
....
612.         conf = fopen(fname, "r");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1754
Status	New

The parse_file method in ravynos-1/archive_read_support_format_mtree.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	ravynos-1/archive_read_support_format_mtree.c	ravynos-1/archive_read_support_format_mtree.c
Line	1253	1253
Object	open	open

Code Snippet

File Name	ravynos-1/archive_read_support_format_mtree.c
Method	parse_file(struct archive_read *a, struct archive_entry *entry,

```
....
1253.                 mtree->fd = open(path, O_RDONLY | O_BINARY |
O_CLOEXEC);
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1755
Status	New

The real_doit method in ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	149	149
Object	open	open

Code Snippet	
File Name	ravynos-1/cxgbetool.c
Method	real_doit(unsigned long cmd, void *data, const char *cmdstr)

```
....
149.                if ((fd = open(buf, O_RDWR)) < 0) {
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1756
Status	New

The loadfw method in ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	1951	1951
Object	open	open

Code Snippet	
File Name	ravynos-1/cxgbetool.c
Method	loadfw(int argc, const char *argv[])

```
....
1951.        fd = open(fname, O_RDONLY);
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1757
Status	New

The loadcfg method in ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	1993	1993
Object	open	open

Code Snippet	
File Name	ravynos-1/cxgbetool.c

Method	loadcfg(int argc, const char *argv[])

```
....
1993.        fd = open(fname, O_RDONLY);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1758
Status	New

The loadboot method in ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2117	2117
Object	open	open

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	loadboot(int argc, const char *argv[])

```
....
2117.        fd = open(fname, O_RDONLY);
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1759
Status	New

The loadbootcfg method in ravynos-1/cxgbetool.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	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	2159	2159
Object	open	open

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	loadbootcfg(int argc, const char *argv[])

```
....
2159.        fd = open(fname, O_RDONLY);
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1760
Status	New

The doit method in ravynos-1/cxgbtool.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	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	136	136
Object	open	open

Code Snippet
File Name ravynos-1/cxgbtool.c
Method doit(const char *iff_name, unsigned long cmd, void *data)

```
....
136.            if ((fd = open(buf, O_RDWR)) < 0)
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1761
Status	New

The load_fw method in ravynos-1/cxgbtool.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	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	999	999
Object	open	open

Code Snippet
File Name ravynos-1/cxgbtool.c
Method load_fw(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
999.        fd = open(fname, O_RDONLY);
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1762
Status	New

The load_boot method in ravynos-1/cxgbtool.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	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1034	1034
Object	open	open

Code Snippet
File Name ravynos-1/cxgbtool.c
Method load_boot(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
1034.       fd = open(fname, O_RDONLY);
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1763
Status	New

The main method in ravynos-1/phttpget.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	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	600	600
Object	open	open

Code Snippet
File Name ravynos-1/phttpget.c
Method main(int argc, char *argv[])

```
....
600.                    fd = open(fname, O_CREAT | O_TRUNC | O_WRONLY,
0644);
```

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=1070095&projectid=70085&pathid=1171
Status	New

The channel_setup_fwd_listener_tcpip method performs a reverse DNS lookup with getnameinfo, at line 3721 of ravynos-1/channels.c. The application then makes a security decision, !=, in ravynos-1/channels.c line 3721, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3799	3801
Object	getnameinfo	!=

Code Snippet
File Name ravynos-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3799.             if (getnameinfo(ai->ai_addr, ai->ai_addrlen, ntop,
sizeof(ntop),
....
3801.                 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=1070095&projectid=70085&pathid=1172
Status	New

The connect_next method performs a reverse DNS lookup with getnameinfo, at line 4522 of ravynos-1/channels.c. The application then makes a security decision, !=, in ravynos-1/channels.c line 4522, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	4539	4541
Object	getnameinfo	!=

Code Snippet
File Name ravynos-1/channels.c
Method connect_next(struct channel_connect *cctx)

```
....
4539.                   if (getnameinfo(cctx->ai->ai_addr, cctx->ai-
>ai_addrlen,
....
4541.                       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=1070095&projectid=70085&pathid=1173
Status	New

The format_listen_addrs method performs a reverse DNS lookup with getnameinfo, at line 2961 of ravynos-1/servconf.c. The application then makes a security decision, !=, in ravynos-1/servconf.c line 2961, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2974	2976
Object	getnameinfo	!=

Code Snippet
File Name ravynos-1/servconf.c
Method format_listen_addrs(struct listenaddr *la)

```
....
2974.             if ((r = getnameinfo(ai->ai_addr, ai->ai_addrlen,
addr,
....
2976.                 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=1070095&projectid=70085&pathid=1174
Status	New

The format_listen_addrs method performs a reverse DNS lookup with getnameinfo, at line 2961 of ravynos-1/servconf.c. The application then makes a security decision, r, in ravynos-1/servconf.c line 2961, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2974	2974
Object	getnameinfo	r

Code Snippet
File Name ravynos-1/servconf.c
Method format_listen_addrs(struct listenaddr *la)

```
....
2974.               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=1070095&projectid=70085&pathid=1175
Status	New

The *endpoint method performs a reverse DNS lookup with getnameinfo, at line 106 of ravynos-1/show.c. The application then makes a security decision, ret, in ravynos-1/show.c line 106, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/show.c	ravynos-1/show.c
Line	120	121
Object	getnameinfo	ret

Code Snippet
File Name ravynos-1/show.c
Method static char *endpoint(const struct sockaddr *addr)

```
....
120.          ret = getnameinfo(addr, addr_len, host, sizeof(host),
service, sizeof(service), NI_DGRAM | NI_NUMERICSERV | NI_NUMERICHOST);
121.          if (ret) {
```

Reliance on DNS Lookups in a Decision\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1176

Status	New

The channel_setup_fwd_listener_tcpip method performs a reverse DNS lookup with getaddrinfo, at line 3721 of ravynos-1/channels.c. The application then makes a security decision, !=, in ravynos-1/channels.c line 3721, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3764	3764
Object	getaddrinfo	!=

Code Snippet
File Name ravynos-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3764.		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=1070095&projectid=70085&pathid=1177
Status	New

The channel_setup_fwd_listener_tcpip method performs a reverse DNS lookup with getaddrinfo, at line 3721 of ravynos-1/channels.c. The application then makes a security decision, r, in ravynos-1/channels.c line 3721, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	3764	3764
Object	getaddrinfo	r

Code Snippet
File Name ravynos-1/channels.c
Method channel_setup_fwd_listener_tcpip(struct ssh *ssh, int type,

```
....
3764.		if ((r = getaddrinfo(addr, strport, &hints, &aitop)) != 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=1070095&projectid=70085&pathid=1178
Status	New

The connect_to_helper method performs a reverse DNS lookup with getaddrinfo, at line 4598 of ravynos-1/channels.c. The application then makes a security decision, !=, in ravynos-1/channels.c line 4598, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	4637	4638
Object	getaddrinfo	!=

Code Snippet
File Name ravynos-1/channels.c
Method connect_to_helper(struct ssh *ssh, const char *name, int port, int socktype,

```
....
4637.           if ((gaierr = getaddrinfo(name, strport, &hints,
&cctx->aitop))
4638.               != 0) {
```

Reliance on DNS Lookups in a Decision\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1179
Status	New

The connect_to_helper method performs a reverse DNS lookup with getaddrinfo, at line 4598 of ravynos-1/channels.c. The application then makes a security decision, gaierr, in ravynos-1/channels.c line 4598, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	4637	4637
Object	getaddrinfo	gaierr

Code Snippet
File Name ravynos-1/channels.c
Method connect_to_helper(struct ssh *ssh, const char *name, int port, int socktype,

```
....
4637.           if ((gaierr = getaddrinfo(name, strport, &hints,
&cctx->aitop))
```

Reliance on DNS Lookups in a Decision\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=1180
Status	New

The x11_create_display_inet method performs a reverse DNS lookup with getaddrinfo, at line 4939 of ravynos-1/channels.c. The application then makes a security decision, !=, in ravynos-1/channels.c line 4939, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	4962	4963
Object	getaddrinfo	!=

Code Snippet
File Name ravynos-1/channels.c
Method x11_create_display_inet(struct ssh *ssh, int x11_display_offset,

```
....
4962.                if ((gaierr = getaddrinfo(NULL, strport,
4963.                    &hints, &aitop)) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1181
Status	New

The x11_create_display_inet method performs a reverse DNS lookup with getaddrinfo, at line 4939 of ravynos-1/channels.c. The application then makes a security decision, gaierr, in ravynos-1/channels.c line 4939, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	4962	4962
Object	getaddrinfo	gaierr

Code Snippet
File Name ravynos-1/channels.c
Method x11_create_display_inet(struct ssh *ssh, int x11_display_offset,

```
....
4962.                if ((gaierr = getaddrinfo(NULL, strport,
```

Reliance on DNS Lookups in a Decision\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=700

	85&pathid=1182
Status	New

The x11_connect_display method performs a reverse DNS lookup with getaddrinfo, at line 5096 of ravynos-1/channels.c. The application then makes a security decision, !=, in ravynos-1/channels.c line 5096, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	5181	5181
Object	getaddrinfo	!=

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

```
....
5181.        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=1070095&projectid=70085&pathid=1183
Status	New

The x11_connect_display method performs a reverse DNS lookup with getaddrinfo, at line 5096 of ravynos-1/channels.c. The application then makes a security decision, gaierr, in ravynos-1/channels.c line 5096, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/channels.c	ravynos-1/channels.c
Line	5181	5181
Object	getaddrinfo	gaierr

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

```
....
5181.        if ((gaierr = getaddrinfo(buf, 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=1070095&projectid=70085&pathid=1184
Status	New

The main method performs a reverse DNS lookup with getaddrinfo, at line 293 of ravynos-1/phttpget.c. The application then makes a security decision, error, in ravynos-1/phttpget.c line 293, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/phttpget.c	ravynos-1/phttpget.c
Line	345	347
Object	getaddrinfo	error

Code Snippet
File Name ravynos-1/phttpget.c
Method main(int argc, char *argv[])

```
....
345.        error = getaddrinfo(env_HTTP_PROXY ? env_HTTP_PROXY :
servername,
....
347.        if (error)
```

Reliance on DNS Lookups in a Decision\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1185
Status	New

The add_one_listen_addr method performs a reverse DNS lookup with getaddrinfo, at line 797 of ravynos-1/servconf.c. The application then makes a security decision, !=, in ravynos-1/servconf.c line 797, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	832	832
Object	getaddrinfo	!=

Code Snippet
File Name ravynos-1/servconf.c
Method add_one_listen_addr(ServerOptions *options, const char *addr,

```
....
832.        if ((gaierr = getaddrinfo(addr, strport, &hints, &aitop)) !=
0)
```

Reliance on DNS Lookups in a Decision\Path 16:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1186
Status	New

The add_one_listen_addr method performs a reverse DNS lookup with getaddrinfo, at line 797 of ravynos-1/servconf.c. The application then makes a security decision, gaierr, in ravynos-1/servconf.c line 797, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	832	832
Object	getaddrinfo	gaierr

Code Snippet
File Name ravynos-1/servconf.c
Method add_one_listen_addr(ServerOptions *options, const char *addr,

```
....
832.          if ((gaierr = getaddrinfo(addr, strport, &hints, &aitop)) !=
0)
```

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=1070095&projectid=70085&pathid=1726
Status	New

The system data read by open_sbuf in the file ravynos-1/buf.c at line 192 is potentially exposed by open_sbuf found in ravynos-1/buf.c at line 192.

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	204	204
Object	perror	perror

Code Snippet
File Name ravynos-1/buf.c

Method	open_sbuf(void)

```
....
204.                perror(sfn);
```

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=1070095&projectid=70085&pathid=1727
Status	New

The system data read by load_server_config in the file ravynos-1/servconf.c at line 2619 is potentially exposed by load_server_config found in ravynos-1/servconf.c at line 2619.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2629	2629
Object	perror	perror

Code Snippet

File Name	ravynos-1/servconf.c
Method	load_server_config(const char *filename, struct sshbuf *conf)

```
....
2629.               perror(filename);
```

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=1070095&projectid=70085&pathid=1728
Status	New

The system data read by show_main in the file ravynos-1/show.c at line 379 is potentially exposed by show_main found in ravynos-1/show.c at line 379.

	Source	Destination
File	ravynos-1/show.c	ravynos-1/show.c
Line	394	394
Object	perror	perror

Code Snippet

File Name	ravynos-1/show.c
Method	int show_main(int argc, const char *argv[])

```
....
394.                    perror("Unable to list interfaces");
```

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=1070095&projectid=70085&pathid=1729
Status	New

The system data read by show_main in the file ravynos-1/show.c at line 379 is potentially exposed by show_main found in ravynos-1/show.c at line 379.

	Source	Destination
File	ravynos-1/show.c	ravynos-1/show.c
Line	430	430
Object	perror	perror

Code Snippet	
File Name	ravynos-1/show.c
Method	int show_main(int argc, const char *argv[])

```
....
430.                    perror("Unable to list interfaces");
```

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=1070095&projectid=70085&pathid=1730
Status	New

The system data read by show_main in the file ravynos-1/show.c at line 379 is potentially exposed by show_main found in ravynos-1/show.c at line 379.

	Source	Destination
File	ravynos-1/show.c	ravynos-1/show.c
Line	443	443
Object	perror	perror

Code Snippet	
File Name	ravynos-1/show.c
Method	int show_main(int argc, const char *argv[])

```
....
443.                    perror("Unable to access interface");
```

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=1070095&projectid=70085&pathid=1731
Status	New

The system data read by get_sbuf_line in the file ravynos-1/buf.c at line 46 is potentially exposed by get_sbuf_line found in ravynos-1/buf.c at line 46.

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	60	60
Object	errno	fprintf

Code Snippet
File Name   ravynos-1/buf.c
Method   get_sbuf_line(line_t *lp)

```
....
60.                 fprintf(stderr, "%s\n", strerror(errno));
```

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=1070095&projectid=70085&pathid=1732
Status	New

The system data read by get_sbuf_line in the file ravynos-1/buf.c at line 46 is potentially exposed by get_sbuf_line found in ravynos-1/buf.c at line 46.

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	68	68
Object	errno	fprintf

Code Snippet
File Name   ravynos-1/buf.c
Method   get_sbuf_line(line_t *lp)

```
....
68.          fprintf(stderr, "%s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1733
Status	New

The system data read by put_sbuf_line in the file ravynos-1/buf.c at line 81 is potentially exposed by put_sbuf_line found in ravynos-1/buf.c at line 81.

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	88	88
Object	errno	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method put_sbuf_line(const char *cs)

```
....
88.          fprintf(stderr, "%s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1734
Status	New

The system data read by put_sbuf_line in the file ravynos-1/buf.c at line 81 is potentially exposed by put_sbuf_line found in ravynos-1/buf.c at line 81.

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	104	104
Object	errno	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method put_sbuf_line(const char *cs)

```
....
104.                    fprintf(stderr, "%s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1735
Status	New

The system data read by put_sbuf_line in the file ravynos-1/buf.c at line 81 is potentially exposed by put_sbuf_line found in ravynos-1/buf.c at line 81.

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	115	115
Object	errno	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method put_sbuf_line(const char *cs)

```
....
115.              fprintf(stderr, "%s\n", strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1736
Status	New

The system data read by close_sbuf in the file ravynos-1/buf.c at line 216 is potentially exposed by close_sbuf found in ravynos-1/buf.c at line 216.

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	220	220
Object	errno	fprintf

Code Snippet
File Name ravynos-1/buf.c
Method close_sbuf(void)

```
....
220.                    fprintf(stderr, "%s: %s\n", sfn,
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1737
Status	New

The system data read by fail in the file ravynos-1/lockstat.c at line 267 is potentially exposed by fail found in ravynos-1/lockstat.c at line 267.

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	270	277
Object	errno	fprintf

Code Snippet
File Name ravynos-1/lockstat.c
Method fail(int do_perror, const char *message, ...)

```
....
270.          int save_errno = errno;
....
277.               (void) fprintf(stderr, ": %s", strerror(save_errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1738
Status	New

The system data read by build_counters_from_header in the file ravynos-1/pmcstudy.c at line 2095 is potentially exposed by build_counters_from_header found in ravynos-1/pmcstudy.c at line 2095.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2105	2105
Object	errno	printf

Code Snippet
File Name ravynos-1/pmcstudy.c
Method build_counters_from_header(FILE *io)

```
....
2105.            printf("First line can't be read from file err:%d\n", 
errno);
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1739
Status	New

The system data read by build_counters_from_header in the file ravynos-1/pmcstudy.c at line 2095 is potentially exposed by build_counters_from_header found in ravynos-1/pmcstudy.c at line 2095.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2131	2131
Object	errno	printf

Code Snippet
File Name ravynos-1/pmcstudy.c
Method build_counters_from_header(FILE *io)

```
....
2131.            printf("No memory err:%d\n", errno);
```

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=1070095&projectid=70085&pathid=1740
Status	New

The system data read by process_file in the file ravynos-1/pmcstudy.c at line 2243 is potentially exposed by process_file found in ravynos-1/pmcstudy.c at line 2243.

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2260	2259
Object	errno	printf

Code Snippet
File Name ravynos-1/pmcstudy.c
Method process_file(char *filename)

```
....
2260.                           filename, errno);
....
2259.                    printf("Can't process file %s err:%d\n",
```

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=1070095&projectid=70085&pathid=1741
Status	New

The system data read by show_main in the file ravynos-1/show.c at line 379 is potentially exposed by show_main found in ravynos-1/show.c at line 379.

	Source	Destination
File	ravynos-1/show.c	ravynos-1/show.c
Line	403	403
Object	errno	fprintf

Code Snippet
File Name	ravynos-1/show.c
Method	int show_main(int argc, const char *argv[])

```
....
403.                            fprintf(stderr, "Unable to access 
interface %s: %s\n", interface, strerror(errno));
```

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=1070095&projectid=70085&pathid=1020
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	661	661
Object	getopt	getopt

Code Snippet
File Name	ravynos-1/gvinum.c

Method	gvinum_detach(int argc, char * const *argv)

```
....
661.         while ((i = getopt(argc, argv, "f")) != -1) {
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1021
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	762	762
Object	getopt	getopt

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_setstate(int argc, char * const *argv)

```
....
762.         while ((i = getopt(argc, argv, "f")) != -1) {
```

Inconsistent Implementations\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1022
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	821	821
Object	getopt	getopt

Code Snippet

File Name	ravynos-1/gvinum.c
Method	gvinum_list(int argc, char * const *argv)

```
....
821.                 while ((j = getopt(argc, argv, "rsvV")) != -1) {
```

Inconsistent Implementations\Path 4:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1023
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	898	898
Object	getopt	getopt

Code Snippet

File Name ravynos-1/gvinum.c

Method gvinum_move(int argc, char * const *argv)

```
....
898.                while ((j = getopt(argc, argv, "f")) != -1) {
```

Inconsistent Implementations\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1024
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	963	963
Object	getopt	getopt

Code Snippet

File Name ravynos-1/gvinum.c

Method gvinum_parityop(int argc, char * const *argv, int rebuild)

```
....
963.          while ((i = getopt(argc, argv, "fv")) != -1) {
```

Inconsistent Implementations\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1025
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c

Line	1021	1021
Object	getopt	getopt

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_rename(int argc, char * const *argv)

```
....
1021.               while ((j = getopt(argc, argv, "r")) != -1) {
```

Inconsistent Implementations\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1026
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1071	1071
Object	getopt	getopt

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_rm(int argc, char * const *argv)

```
....
1071.         while ((j = getopt(argc, argv, "rf")) != -1) {
```

Inconsistent Implementations\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1027
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1115	1115
Object	getopt	getopt

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_resetconfig(int argc, char * const *argv)

```
....
1115.        while ((i = getopt(argc, argv, "f")) != -1) {
```

Inconsistent Implementations\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1028
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	1186	1186
Object	getopt	getopt

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_start(int argc, char * const *argv)

```
....
1186.        while ((j = getopt(argc, argv, "S")) != -1) {
```

Inconsistent Implementations\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1029
Status	New

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1152	1152
Object	getopt	getopt

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

```
....
1152.        while ((c = getopt(argc, argv, LOCKSTAT_OPTSTR)) !=
GETOPT_EOF) {
```

Inconsistent Implementations\Path 11:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1030
Status	New

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1448	1448
Object	getopt	getopt

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

```
....
1448.        while ((c = getopt(argc, argv, LOCKSTAT_OPTSTR)) !=
GETOPT_EOF) {
```

Inconsistent Implementations\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1031
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2814	2814
Object	getopt	getopt

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

```
....
2814.        while ((i = getopt(argc, argv, "ALHhvm:i:?e:TE:")) != -1) {
```

Inconsistent Implementations\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1032
Status	New

	Source	Destination
File	ravynos-1/rtadvctl.c	ravynos-1/rtadvctl.c

Line	159	159
Object	getopt	getopt

Code Snippet
File Name ravynos-1/rtadvctl.c
Method main(int argc, char *argv[])

```
....
159.        while ((ch = getopt(argc, argv, "Dv")) != -1) {
```

Heuristic Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic Buffer Overflow malloc Version:0

Categories

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

Description

Heuristic Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1397
Status	New

The size of the buffer used by read_mem in len, at line 2059 of ravynos-1/cxgbetool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 3666 of ravynos-1/cxgbetool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3666	2066
Object	argv	len

Code Snippet
File Name ravynos-1/cxgbetool.c
Method main(int argc, const char *argv[])

```
....
3666.  main(int argc, const char *argv[])
```

File Name ravynos-1/cxgbetool.c
Method read_mem(uint32_t addr, uint32_t len, void (*output)(uint32_t *, uint32_t))

```
....
2066.        mr.data = malloc(mr.len);
```

Heuristic Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1398
Status	New

The size of the buffer used by dump_mc7 in len, at line 949 of ravynos-1/cxgbtool.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1744 of ravynos-1/cxgbtool.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/cxgbtool.c	ravynos-1/cxgbtool.c
Line	1744	970
Object	argv	len

Code Snippet

File Name ravynos-1/cxgbtool.c

Method main(int argc, char *argv[])

```
....
1744.  main(int argc, char *argv[])
```

▼

File Name ravynos-1/cxgbtool.c

Method dump_mc7(int argc, char *argv[], int start_arg, const char *iff_name)

```
....
970.         mem.buf = malloc(len);
```

Heuristic Buffer Overflow malloc\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1399
Status	New

The size of the buffer used by xmalloc in len, at line 49 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2021 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	2021	56

Object	argv	len

Code Snippet
File Name ravynos-1/test_x509.c
Method main(int argc, const char *argv[])

```
....
2021.  main(int argc, const char *argv[])
```

File Name ravynos-1/test_x509.c

Method xmalloc(size_t len)

```
....
56.    buf = malloc(len);
```

Heuristic Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1400
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	758
Object	getenv	cp

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name ravynos-1/http.c

Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
758.         char *key = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1401
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	758
Object	getenv	cp

Code Snippet

File Name ravynos-1/http.c

Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name ravynos-1/http.c

Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
758.         char *key = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1402
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1760	758
Object	getenv	cp

Code Snippet

File Name ravynos-1/http.c

Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1760.             if ((p = getenv("HTTP_USER_AGENT")) != NULL) {
```

File Name ravynos-1/http.c

Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
758.          char *key = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1403
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	759
Object	getenv	cp

Code Snippet

File Name ravynos-1/http.c

Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.         if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name ravynos-1/http.c

Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
759.          char *value = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1404
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	759
Object	getenv	cp

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.         if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name ravynos-1/http.c

Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
759.          char *value = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1405
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1760	759
Object	getenv	cp

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1760.               if ((p = getenv("HTTP_USER_AGENT")) != NULL) {
```

File Name	ravynos-1/http.c
Method	http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
759.        char *value = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1406
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	760
Object	getenv	cp

Code Snippet

File Name	ravynos-1/http.c
Method	http_get_proxy(struct url * url, const char *flags)

```
....
1511.       if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

File Name	ravynos-1/http.c
Method	http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
760.        char *buf = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1407
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_get_proxy passes to getenv, at line 1502 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination

File	ravynos-1/http.c	ravynos-1/http.c
Line	1511	760
Object	getenv	cp

Code Snippet
File Name ravynos-1/http.c
Method http_get_proxy(struct url * url, const char *flags)

```
....
1511.        if (((p = getenv("HTTP_PROXY")) || (p =
getenv("http_proxy"))) &&
```

▼

File Name ravynos-1/http.c

Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
760.         char *buf = malloc(strlen(cp) + 1);
```

Heuristic Buffer Overflow malloc\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1408
Status	New

The size of the buffer used by http_parse_authenticate in cp, at line 754 of ravynos-1/http.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that http_request_body passes to getenv, at line 1585 of ravynos-1/http.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/http.c	ravynos-1/http.c
Line	1760	760
Object	getenv	cp

Code Snippet
File Name ravynos-1/http.c
Method http_request_body(struct url *URL, const char *op, struct url_stat *us,

```
....
1760.                if ((p = getenv("HTTP_USER_AGENT")) != NULL) {
```

▼

File Name ravynos-1/http.c

Method http_parse_authenticate(const char *cp, http_auth_challenges_t *cs)

```
....
760.        char *buf = malloc(strlen(cp) + 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=1070095&projectid=70085&pathid=1714
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1516	1516
Object	inc	inc

Code Snippet
File Name ravynos-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 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1715
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1585	1585
Object	in	in

Code Snippet
File Name ravynos-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 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1716
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	1733	1733
Object	out	out

Code Snippet

File Name ravynos-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 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1717
Status	New

	Source	Destination
File	ravynos-1/authzone.c	ravynos-1/authzone.c
Line	5147	5147
Object	out	out

Code Snippet

File Name ravynos-1/authzone.c

Method auth_zone_write_chunks(struct auth_xfer* xfr, const char* fname)

```
....
5147.         out = fopen(fname, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1718
Status	New

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	3386	3386
Object	fp	fp

Code Snippet

File Name ravynos-1/cxgbetool.c

Method parse_offload_policy(const char *fname, struct t4_offload_policy *op)

```
....
3386.        fp = fopen(fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1719
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	199	199
Object	tmp	tmp

Code Snippet

File Name ravynos-1/gvinum.c

Method gvinum_create(int argc, char * const *argv)

```
....
199.                    if ((tmp = fopen(argv[i], "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1720
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c

Line	233	233
Object	tmp	tmp

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
233.                if ((tmp = fopen(tmpfile, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1721
Status	New

	Source	Destination
File	ravynos-1/lockstat.c	ravynos-1/lockstat.c
Line	1330	1330
Object	out	out

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

```
....
1330.                        if ((out = fopen(optarg, "w")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1722
Status	New

	Source	Destination
File	ravynos-1/pmcstudy.c	ravynos-1/pmcstudy.c
Line	2257	2257
Object	io	io

Code Snippet
File Name ravynos-1/pmcstudy.c
Method process_file(char *filename)

```
....
2257.                   io = fopen(filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1723
Status	New

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	2628	2628
Object	f	f

Code Snippet
File Name ravynos-1/servconf.c
Method load_server_config(const char *filename, struct sshbuf *conf)

```
....
2628.         if ((f = fopen(filename, "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=1070095&projectid=70085&pathid=1724
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	450	450
Object	f	f

Code Snippet
File Name ravynos-1/test_x509.c
Method read_file(const char *name, size_t *len)

```
....
450.          f = fopen(name, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1725
Status	New

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	612	612
Object	conf	conf

Code Snippet
File Name ravynos-1/test_x509.c
Method conf_init(const char *fname)

```
....
612.        conf = fopen(fname, "r");
```

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=1070095&projectid=70085&pathid=1162
Status	New

The buffer allocated by <= in ravynos-1/archive_read_support_format_rar.c at line 3621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/archive_read_support_format_rar.c	ravynos-1/archive_read_support_format_rar.c
Line	3630	3630
Object	<=	<=

Code Snippet
File Name ravynos-1/archive_read_support_format_rar.c
Method execute_filter_e8(struct rar_filter *filter, struct rar_virtual_machine *vm, size_t pos, int e9also)

```
....
3630.     for (i = 0; i <= length - 5; i++)
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1163
Status	New

The buffer allocated by <= in ravynos-1/csqrt_test.c at line 256 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/csqrt_test.c	ravynos-1/csqrt_test.c
Line	274	274
Object	<=	<=

Code Snippet

File Name	ravynos-1/csqrt_test.c
Method	test_precision(int maxexp, int mantdig)

```
....
274.          for (exp = 0; exp <= maxexp; exp += 2) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1164
Status	New

The buffer allocated by <= in ravynos-1/cxgbetool.c at line 1115 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/cxgbetool.c	ravynos-1/cxgbetool.c
Line	1129	1129
Object	<=	<=

Code Snippet

File Name	ravynos-1/cxgbetool.c
Method	set_filter(uint32_t idx, int argc, const char *argv[], int hash)

```
....
1129.        for (start_arg = 0; start_arg + 2 <= argc; start_arg += 2) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1165
Status	New

The buffer allocated by <= in ravynos-1/dp_rx.c at line 900 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	907	907
Object	<=	<=

Code Snippet
File Name ravynos-1/dp_rx.c
Method void ath11k_peer_frags_flush(struct ath11k *ar, struct ath11k_peer *peer)

```
....
907.        for (i = 0; i <= IEEE80211_NUM_TIDS; i++) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1166
Status	New

The buffer allocated by <= in ravynos-1/dp_rx.c at line 918 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	925	925
Object	<=	<=

Code Snippet
File Name ravynos-1/dp_rx.c
Method void ath11k_peer_rx_tid_cleanup(struct ath11k *ar, struct ath11k_peer *peer)

```
....
925.         for (i = 0; i <= IEEE80211_NUM_TIDS; 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=1070095&projectid=70085&pathid=1167
Status	New

The buffer allocated by <= in ravynos-1/dp_rx.c at line 1160 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	1211	1211
Object	<=	<=

Code Snippet
File Name ravynos-1/dp_rx.c
Method int ath11k_dp_peer_rx_pn_replay_config(struct ath11k_vif *arvif,

```
....
1211.        for (tid = 0; tid <= IEEE80211_NUM_TIDS; tid++) {
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1168
Status	New

The buffer allocated by <= in ravynos-1/dp_rx.c at line 3152 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/dp_rx.c	ravynos-1/dp_rx.c
Line	3173	3173
Object	<=	<=

Code Snippet
File Name ravynos-1/dp_rx.c
Method int ath11k_peer_rx_frag_setup(struct ath11k *ar, const u8 *peer_mac, int vdev_id)

```
....
3173.         for (i = 0; i <= IEEE80211_NUM_TIDS; i++) {
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1169
Status	New

The buffer allocated by <= in ravynos-1/if_bge.c at line 3138 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/if_bge.c	ravynos-1/if_bge.c
Line	3147	3147
Object	<=	<=

Code Snippet
File Name ravynos-1/if_bge.c
Method bge_has_multiple_ports(struct bge_softc *sc)

```
....
3147.         for (fscan = 0; fscan <= PCI_FUNCMAX; fscan++)
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1170
Status	New

The buffer allocated by <= in ravynos-1/iptests.c at line 900 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	932	932
Object	<=	<=

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test5(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
932.                for (i = 0; i <=
(TH_URG|TH_ACK|TH_PUSH|TH_RST|TH_SYN|TH_FIN);
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1033
Status	New

Method ip_test7 at line 1322 of ravynos-1/iptests.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	1345	1345
Object	rand	rand

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test7(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
1345.                    *s = (rand() >> 13) & 0xff;
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1034
Status	New

Method ip_test7 at line 1322 of ravynos-1/iptests.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination

File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	1360	1360
Object	rand	rand

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test7(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
1360.                      *s = (rand() >> 13) & 0xff;
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1035
Status	New

Method ip_test1 at line 99 of ravynos-1/iptests.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	341	341
Object	rand	rand

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test1(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
341.                 if ((rand() & 0x1f) != 0) {
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1036
Status	New

Method ip_test1 at line 99 of ravynos-1/iptests.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c

Line	351	351
Object	rand	rand

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test1(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
351.                        if ((rand() & 0x1f) != 0) {
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1037
Status	New

Method ip_test1 at line 99 of ravynos-1/iptests.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	361	361
Object	rand	rand

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test1(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
361.                if ((rand() & 0x1f) != 0) {
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1038
Status	New

Method ip_test7 at line 1322 of ravynos-1/iptests.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	1339	1339

Object	srand	srand

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test7(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
1339.        srand(time(NULL) ^ (getpid() * getppid()));
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1039
Status	New

Method ip_test1 at line 99 of ravynos-1/iptests.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	ravynos-1/iptests.c	ravynos-1/iptests.c
Line	297	297
Object	srand	srand

Code Snippet
File Name ravynos-1/iptests.c
Method ip_test1(char *dev, int mtu, ip_t *ip, struct in_addr gwip, int ptest)

```
....
297.             srand(tv.tv_sec ^ getpid() ^ tv.tv_usec);
```

Heuristic 2nd Order Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow malloc Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1366
Status	New

The size of the buffer used by xmalloc in len, at line 49 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	651	56
Object	fgetc	len

Code Snippet
File Name	ravynos-1/test_x509.c
Method	conf_next_low(void)

```
....
651.                  x = fgetc(conf);
```

▼

File Name	ravynos-1/test_x509.c
Method	xmalloc(size_t len)

```
....
56.     buf = malloc(len);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1367
Status	New

The size of the buffer used by xmalloc in len, at line 49 of ravynos-1/test_x509.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that conf_next_low passes to fgetc, at line 643 of ravynos-1/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	ravynos-1/test_x509.c	ravynos-1/test_x509.c
Line	657	56
Object	fgetc	len

Code Snippet
File Name	ravynos-1/test_x509.c
Method	conf_next_low(void)

```
....
657.                  x = fgetc(conf);
```

▼

File Name	ravynos-1/test_x509.c

Method	xmalloc(size_t len)

```
....
56.    buf = malloc(len);
```

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=1070095&projectid=70085&pathid=1438
Status	New

	Source	Destination
File	ravynos-1/buf.c	ravynos-1/buf.c
Line	200	200
Object	mkstemp	mkstemp

Code Snippet

File Name	ravynos-1/buf.c
Method	open_sbuf(void)

```
....
200.        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=1070095&projectid=70085&pathid=1439
Status	New

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	210	210
Object	mkstemp	mkstemp

Code Snippet

File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
210.                if ((fd = mkstemp(tmpfile)) == -1) {
```

Privacy Violation

Query Path:
CPP\Cx\CPP Low Visibility\Privacy Violation Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Privacy Violation\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1040
Status	New

Method dump_config at line 3000 of ravynos-1/servconf.c sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	ravynos-1/servconf.c	ravynos-1/servconf.c
Line	3124	2952
Object	auth_methods	printf

Code Snippet
File Name ravynos-1/servconf.c
Method dump_config(ServerOptions *o)

```
....
3124.           o->num_auth_methods, o->auth_methods);
```

File Name ravynos-1/servconf.c
Method dump_cfg_strarray_oneline(ServerOpCodes code, u_int count, char **vals)

```
....
2952.               printf(" %s",  vals[i]);
```

Leaving Temporary Files

Query Path:
CPP\Cx\CPP Low Visibility\Leaving Temporary Files Version:0

Categories

OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Leaving Temporary Files\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1440
Status	New

The application generates a temporary file mkstemp, in the gvinum_create method at ravynos-1/gvinum.c:175. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	ravynos-1/gvinum.c	ravynos-1/gvinum.c
Line	210	210
Object	mkstemp	mkstemp

Code Snippet
File Name ravynos-1/gvinum.c
Method gvinum_create(int argc, char * const *argv)

```
....
210.                if ((fd = mkstemp(tmpfile)) == -1) {
```

Information Exposure Through Comments

Query Path:
CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description

Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1070095&projectid=70085&pathid=1764
Status	New

	Source	Destination
File	ravynos-1/camcontrol.c	ravynos-1/camcontrol.c
Line	2454	2454
Object	pwd-	pwd-

Code Snippet

File Name	ravynos-1/camcontrol.c
Method	/* pwd->password may not be null terminated */

```
....
                /* pwd->password may not be null terminated */
```

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 boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow OutOfBound

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CGI Stored XSS

Risk

What might happen

Stored malicious data might retrieve system information and exploit the system through CGI (Common Gateway Interface).

Cause

How does it happen

The CGI specification provides opportunities to read files, acquire shell access, and corrupt file systems on server machines and their attached hosts.

Means of gaining access include: exploiting assumptions of the script, exploiting weaknesses in the server environment, and exploiting weaknesses in other programs and system calls.

The primary weakness in CGI scripts is insufficient input validation.

General Recommendations

How to avoid it

Do not provide unnecessary file permissions.

Validate and encode all DB output.

Source Code Examples

Perl

Bad - Printing out data from BD without encoding

```
#!/usr/bin/perl
use CGI;
use DBI;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", @row),
      $cgi->end_html;
```

Good - Printing out from DB after encoding

```
#!/usr/bin/perl
use CGI;
use DBI;
use HTML::Entities;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", HTML::Entities::encode(@row)),
      $cgi->end_html;
```

Command Injection

Risk

What might happen

An attacker could run arbitrary system-level OS commands on the application server host. Depending on the application's OS permissions, these could include:

- File actions (read / create / modify / delete)
- Open a network connection to the attacker's server
- Start and stop system services
- Modify the running application
- Complete server takeover

Cause

How does it happen

The application runs an OS system-level command to complete it's task, rather than via the application code. The command includes untrusted data, that may be controllable by an attacker. This untrusted string may contain malicious system-level commands engineered by an attacker, which could be executed as though the attacker were running commands directly on the application server.

In this case, the application receives data from the user input, and passes it as a string to the Operating System. This unvalidated data is then executed by the OS as a system command, running with the same system privileges as the application.

General Recommendations

How to avoid it

- Refactor the code to avoid any direct shell command execution. Instead, use platform provided APIs or library calls.
- If it is impossible to remove the command execution, execute only static commands that do not include dynamic, user-controlled data.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified format, rather than rejecting bad patterns (blacklist). Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
- In order to minimize damage as a measure of defense in depth, configure the application to run using a restricted user account that has no unnecessary OS privileges.
- If possible, isolate all OS commands to use a separate dedicated user account that has minimal privileges only for the specific commands and files used by the application, according to the Principle of Least Privilege.

- If absolutely necessary to call a system command or execute external program with user input, do not concatenate the user input with the command. Instead, isolate the parameters from the command by using a platform function that supports this.

- Do not call `system()` or it's variants, as this does not support separating data parameters from the system command.
- Instead, use one of the functions that receive arguments separately from the command, and validates them. This includes `ShellExecute()`, `execve()`, or one of it's variants.
- It is very important to pass user-controlled data to the function as the `lpParameters` or `argN` argument (or equivalent), and ensure that it is properly quoted. Never pass user controlled data to as the first parameter for `cmdname` or `filePath`.
- Do not directly execute any shell or command interpreters, such as `bash`, `cmd`, or `make`, with user-controlled input.

Source Code Examples

CPP

Execute System (Shell) Command With User Input

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
            result = system(argv[1]);
      }
      return result;
}
```

Call External Program with Safe Parameters

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
            char* param = escapeArg(argv[1]);

            result = _spawnl(_P_WAIT, EXTERNAL_PROGRAM_PATH, EXTERNAL_PROGRAM_PATH, param,
NULL);
      }
      return result;
}
```

Refactor Code to Use API Function

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
            char* param = escapeArg(argv[1]);

            result = performSpecificAction(param);
      }
      return result;
}
```

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

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```java
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

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

Long 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

Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;
  void setPassword()
```

```
    {
        password = System.console().readLine("Enter your password: ");
     }
  }
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n'){
                   password[i]='\0';
                   break;
             } else{
                   password[i++]=ch;
                   fflush(0);
             }
      }
      i=0;
      memset(password,'\0',256);
}

int main()

{

      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n')
                   break;
      }
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

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 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));
    }
}
```

Stored Buffer Overflow cpycat

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 Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.

- Some implementations of the function carry significant security risks.

- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		

Previous Entry Names	
Change Date	**Previous Entry Name**
2008-04-11	Inconsistent Implementations

BACK TO TOP

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.

Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

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';
```

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 malloc

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Heuristic Buffer Overflow malloc

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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

Leaving Temporary Files

Risk

What might happen

Applications often create temporary files containing sensitive business data or personal information, in order to handle the file generation process in several steps, or even as the output of an automatic process. These files, if left exposed on disk for an indeterminate period of time, could leak the secret data to unauthorized users.

Cause

How does it happen

It is very common for applications to use temporary files, as intermediate storage and to aid with processing large amounts of data or long-running calculations. Applications require such files so frequently that most operating systems allocate a dedicated area for temporary files, such as a TEMP directory, and several different mechanisms for creating them exist in most platforms. However, by default these temporary files are not deleted automatically, and will remain on disk indefinitely. If the program does not explicitly and proactively delete the temporary files when it is finished processing them, they might be accessbile to other users of the computer.

General Recommendations

How to avoid it

- Always explicitly delete any temporary file created. Ensure temp file deletion will occur by wrapping it in a `finally { }` block, or call `File.deleteOnExit()` to ensure eventual deletion.
- Additionally, to ensure that all temporary files will eventually be deleted, consider implementing additional functionality that will periodically scrape and delete all unused, existing temporary files.
- Ensure all existing file handles or references are closed before attempting deletion.

Source Code Examples

Java

Leaving Temporary Report File

```
private byte[] generateData(int key) {
      File tempFile = File.createTempFile(TEMP_PREFIX, ".txt");

      FileOutputStream writer = new FileOutputStream(tempFile);
      ReportGenerator.writeHugeReportToFileStream(writer, key);

      FileInputStream reader = new FileInputStream(tempFile);
      int length = reader.available();
      if (length > 0) {
            byte[] reportData = new byte[length];
            reader.read(reportData);

            return reportData;
     }
      else {
            return null;
     }
}
```

Cleaning Up Temporary Report File

```
private byte[] generateData(int key) {
      byte[] reportData = null;
      File tempFile = null;
      FileOutputStream writer = null;
      FileInputStream reader = null;

      try {
      tempFile = File.createTempFile(TEMP_PREFIX, ".txt");

      writer = new FileOutputStream(tempFile);
      ReportGenerator.writeHugeReportToFileStream(writer, key);

      reader = new FileInputStream(tempFile);
      int length = reader.available();
      if (length > 0) {
              reportData = new byte[length];
          reader.read(reportData);
      }
    }
      catch (IOException e) {
            handleError(e);
    }
      finally {
            if (reader != null) {
            try {
                   reader.close();
            }
                   catch (IOException e) {
                          handleError(e);
            }
        }

            if (writer != null) {
            try {
                   writer.close();
            }
            catch (IOException e) {
                handleError(e);
            }
        }

            if (tempFile != null) {
            try {
            tempFile.delete();
            }
            catch (IOException e) {
                handleError(e);
            }
        }
    }
      return reportData;
}
```

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

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 updated Time of Introduction	Cigital	External
2008-08-01	added/updated white box definitions	KDM Analytics	External
2008-09-08	CWE Content Team updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2008-11-24	CWE Content Team updated Relationships, Taxonomy Mappings	MITRE	Internal
2009-03-10	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2009-12-28	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2010-02-16	CWE Content Team updated Relationships	MITRE	Internal

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