RetroArch Scan Report

Project Name	RetroArch
Scan Start	Friday, June 21, 2024 12:22:33 AM
Preset	Checkmarx Default
Scan Time	00h:17m:56s
Lines Of Code Scanned	135916
Files Scanned	57
Report Creation Time	Friday, June 21, 2024 10:40:39 AM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (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

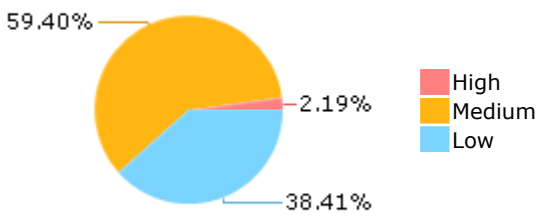
Results Limit

Results limit per query was set to 50

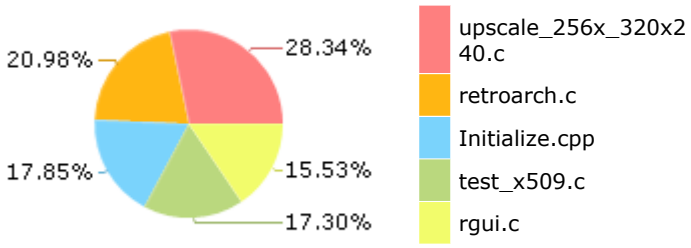
Selected Queries

Selected queries are listed in Result Summary

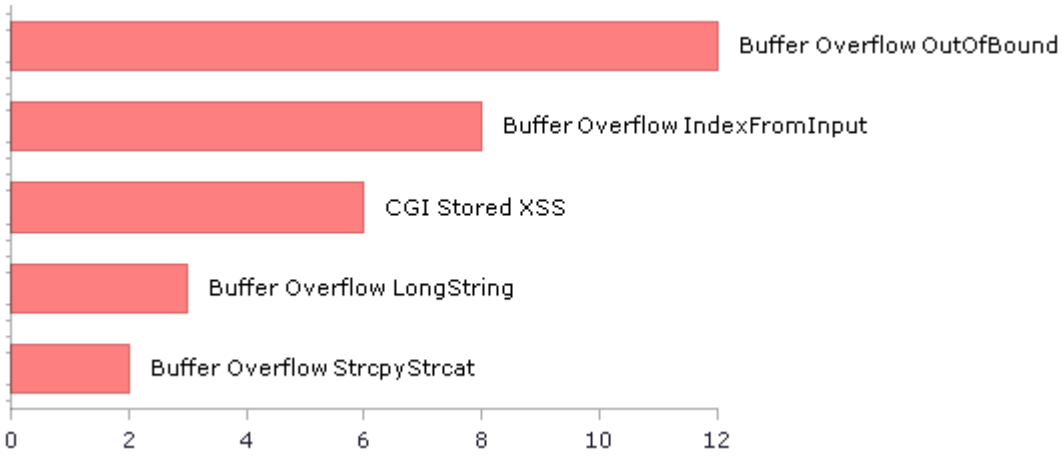
Result Summary



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	247	163
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	132	132
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	30	30
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	0	0
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	6	1
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	292	292
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	6	1
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
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	292	292
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	27	27
PCI DSS (3.2) - 6.5.2 - Buffer overflows	138	124
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)	6	1
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	10	10
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.	3	3
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.	0	0
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.	122	122
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.	30	30
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.	18	13

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	132	132
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	27	27
SC-4 Information in Shared Resources (P1)	3	3
SC-5 Denial of Service Protection (P1)*	419	160
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	108	63
SI-11 Error Handling (P2)*	252	252
SI-15 Information Output Filtering (P0)	6	1
SI-16 Memory Protection (P1)	27	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 - 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

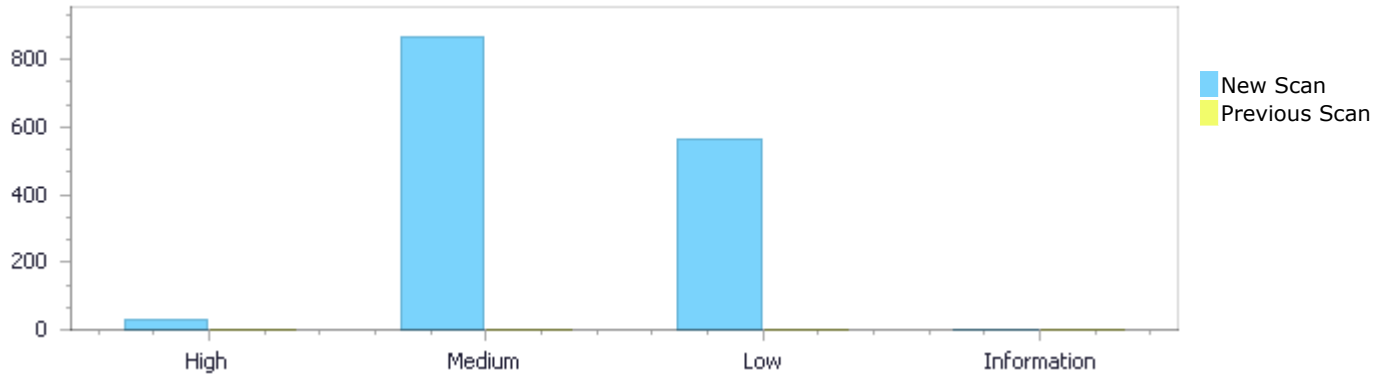
Scan Summary - Custom

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	32	869	562	0	1,463
Recurrent Issues	0	0	0	0	0
Total	32	869	562	0	1,463
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	32	869	562	0	1,463
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	32	869	562	0	1,463

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow OutOfBound	12	High
Buffer Overflow IndexFromInput	8	High
CGI Stored XSS	6	High
Buffer Overflow LongString	3	High
Buffer Overflow StrcpyStrcat	2	High

Buffer Overflow boundedcpy	1	High
Dangerous Functions	292	Medium
Use of Uninitialized Variable	201	Medium
Buffer Overflow boundcpy WrongSizeParam	99	Medium
Use of Zero Initialized Pointer	83	Medium
Memory Leak	80	Medium
Stored Buffer Overflow boundcpy	38	Medium
Wrong Size t Allocation	31	Medium
MemoryFree on StackVariable	20	Medium
Integer Overflow	10	Medium
Char Overflow	4	Medium
Divide By Zero	4	Medium
Heap Inspection	3	Medium
Buffer Overflow AddressOfLocalVarReturned	2	Medium
Float Overflow	2	Medium
Unchecked Return Value	252	Low
Improper Resource Access Authorization	122	Low
NULL Pointer Dereference	50	Low
Unchecked Array Index	31	Low
Potential Off by One Error in Loops	27	Low
Use of Insufficiently Random Values	27	Low
Sizeof Pointer Argument	17	Low
Incorrect Permission Assignment For Critical Resources	10	Low
TOCTOU	10	Low
Use of Sizeof On a Pointer Type	6	Low
Arithmenic Operation On Boolean	3	Low
Heuristic 2nd Order Buffer Overflow malloc	2	Low
Inconsistent Implementations	2	Low
Potential Precision Problem	2	Low
Heuristic Buffer Overflow malloc	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
RetroArch/upscale_256x_320x240.c	208
RetroArch/rgui.c	81
RetroArch/retroarch.c	76
RetroArch/models.c	61
RetroArch/xmb.c	58
RetroArch/test_x509.c	56
RetroArch/config_file.c	47
RetroArch/rc_api_common.c	36
RetroArch/net_http.c	33
RetroArch/shader_glsl.c	30

Scan Results Details

Buffer Overflow OutOfBound

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

Categories

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

Description

Buffer Overflow OutOfBound\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=122
Status	New

The size of the buffer used by gl_glsl_set_coords in size, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1604
Object	attribs	size

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1604.        gl_glsl_set_coord_array(attribs, uni->tex_coord,
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=123
Status	New

The size of the buffer used by gl_glsl_set_coords in loc, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1604
Object	attribs	loc

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1604.        gl_glsl_set_coord_array(attribs, uni->tex_coord,
```

Buffer Overflow OutOfBound\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=124
Status New

The size of the buffer used by gl_glsl_set_coords in offset, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1604
Object	attribs	offset

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1604.        gl_glsl_set_coord_array(attribs, uni->tex_coord,
```

Buffer Overflow OutOfBound\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=125
Status New

The size of the buffer used by gl_glsl_set_coords in loc, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1611
Object	attribs	loc

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1611.        gl_glsl_set_coord_array(attribs, uni->vertex_coord,
```

Buffer Overflow OutOfBound\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=126
Status New

The size of the buffer used by gl_glsl_set_coords in size, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1611
Object	attribs	size

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1611.        gl_glsl_set_coord_array(attribs, uni->vertex_coord,
```

Buffer Overflow OutOfBound\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=100

	11&pathid=127
Status	New

The size of the buffer used by gl_glsl_set_coords in offset, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1611
Object	attribs	offset

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1611.        gl_glsl_set_coord_array(attribs, uni->vertex_coord,
```

Buffer Overflow OutOfBound\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=128
Status	New

The size of the buffer used by gl_glsl_set_coords in loc, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1618
Object	attribs	loc

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1618.        gl_glsl_set_coord_array(attribs, uni->color,
```

Buffer Overflow OutOfBound\Path 8:

Severity	High

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=129
Status	New

The size of the buffer used by gl_glsl_set_coords in size, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1618
Object	attribs	size

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1618.        gl_glsl_set_coord_array(attribs, uni->color,
```

Buffer Overflow OutOfBound\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=130
Status	New

The size of the buffer used by gl_glsl_set_coords in offset, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1618
Object	attribs	offset

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1618.        gl_glsl_set_coord_array(attribs, uni->color,
```

Buffer Overflow OutOfBound\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=131
Status	New

The size of the buffer used by gl_glsl_set_coords in loc, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1625
Object	attribs	loc

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1625.        gl_glsl_set_coord_array(attribs, uni->lut_tex_coord,
```

Buffer Overflow OutOfBound\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=132
Status	New

The size of the buffer used by gl_glsl_set_coords in size, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1625
Object	attribs	size

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1625.        gl_glsl_set_coord_array(attribs, uni->lut_tex_coord,
```

Buffer Overflow OutOfBound\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=133
Status	New

The size of the buffer used by gl_glsl_set_coords in offset, at line 1555 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_set_coords passes to attribs, at line 1555 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1559	1625
Object	attribs	offset

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1559.     struct glsl_attrib attribs[4];
....
1625.        gl_glsl_set_coord_array(attribs, uni->lut_tex_coord,
```

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=1010010&projectid=10011&pathid=5
Status	New

The size of the buffer used by SB_append_char in PostfixExpr, at line 126 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	651	129
Object	fgetc	PostfixExpr

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/test_x509.c
Method SB_append_char(string_builder *sb, int c)

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

Buffer Overflow IndexFromInput\Path 2:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=6
Status New

The size of the buffer used by SB_append_char in PostfixExpr, at line 126 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	657	129
Object	fgetc	PostfixExpr

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/test_x509.c
Method SB_append_char(string_builder *sb, int c)

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

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=7
Status	New

The size of the buffer used by *string_list_new_special in zone_desc_len, at line 1443 of RetroArch/retroarch.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *string_list_new_special passes to zone_desc, at line 1443 of RetroArch/retroarch.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	1623	1629
Object	zone_desc	zone_desc_len

Code Snippet
File Name RetroArch/retroarch.c
Method struct string_list *string_list_new_special(enum string_list_type type,

```
....
1623.                  while (fgets(zone_desc, TIMEZONE_LENGTH,
zones_file))
....
1629.                           zone_desc[zone_desc_len] = '\0';
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=8
Status	New

The size of the buffer used by load_wavefront_obj in num_materials, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	247
Object	line	num_materials

Code Snippet

File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
247.           if (sscanf(s, "usemtl %s", /*MAX_MATERIAL_NAME-1,
*/model->material[m->num_materials].name) == 1) {
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=9
Status	New

The size of the buffer used by load_wavefront_obj in num_materials, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	247
Object	BinaryExpr	num_materials

Code Snippet	
File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
247.           if (sscanf(s, "usemtl %s", /*MAX_MATERIAL_NAME-1,
*/model->material[m->num_materials].name) == 1) {
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=10
Status	New

The size of the buffer used by run_test_case in u, at line 1442 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c

Line	423	1505
Object	BinaryExpr	u

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

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

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1505.             certs[u].data = read_file(tc->cert_names[u],
&certs[u].len);
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=11
Status	New

The size of the buffer used by run_test_case in u, at line 1442 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	423	1570
Object	BinaryExpr	u

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

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

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1570.                   ctx.vtable->append(&ctx.vtable, certs[u].data +
v, w);
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=12
Status	New

The size of the buffer used by run_test_case in u, at line 1442 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	423	1634
Object	BinaryExpr	u

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

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

File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1634.             xfree(certs[u].data);
```

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=1010010&projectid=10011&pathid=116
Status	New

Unvalidated DB output was found in line number 208 in RetroArch/models.c file. A possible XSS exploitation was found in printf at line number 208.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	256
Object	line	printf

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
256.           } else { printf("%s", s); vc_assert(0); }
```

CGI Stored XSS\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=117
Status	New

Unvalidated DB output was found in line number 208 in RetroArch/models.c file. A possible XSS exploitation was found in printf at line number 208.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	306
Object	line	printf

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
306.           } else { printf("%s", s); vc_assert(0); }
```

CGI Stored XSS\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=118
Status	New

Unvalidated DB output was found in line number 208 in RetroArch/models.c file. A possible XSS exploitation was found in printf at line number 208.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	309
Object	line	printf

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
309.           printf("%02x %02x %s", s[0], s[1], s); vc_assert(0);
break;
```

CGI Stored XSS\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=119
Status	New

Unvalidated DB output was found in line number 208 in RetroArch/models.c file. A possible XSS exploitation was found in printf at line number 208.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	256
Object	BinaryExpr	printf

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
256.           } else { printf("%s", s); vc_assert(0); }
```

CGI Stored XSS\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=120
Status	New

Unvalidated DB output was found in line number 208 in RetroArch/models.c file. A possible XSS exploitation was found in printf at line number 208.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	306
Object	BinaryExpr	printf

Code Snippet

File Name RetroArch/models.c

Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
306.           } else { printf("%s", s); vc_assert(0); }
```

CGI Stored XSS\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=121
Status	New

Unvalidated DB output was found in line number 208 in RetroArch/models.c file. A possible XSS exploitation was found in printf at line number 208.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	309
Object	BinaryExpr	printf

Code Snippet

File Name RetroArch/models.c

Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
309.           printf("%02x %02x %s", s[0], s[1], s); vc_assert(0);
break;
```

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=1010010&projectid=10011&pathid=1
Status	New

The size of the buffer used by config_set_char in buf, at line 1382 of RetroArch/config_file.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that config_set_char passes to "%c", at line 1382 of RetroArch/config_file.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1385	1386
Object	"%c"	buf

Code Snippet	
File Name	RetroArch/config_file.c
Method	void config_set_char(config_file_t *conf, const char *key, char val)

```
....
1385.     snprintf(buf, sizeof(buf), "%c", val);
1386.     config_set_string(conf, key, buf);
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=2
Status	New

The size of the buffer used by gl_glsl_compile_shader in source, at line 349 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_compile_program passes to "#define FRAGMENT\n#define PARAMETER_UNIFORM\n", at line 453 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	492	405
Object	"#define FRAGMENT\n#define PARAMETER_UNIFORM\n"	source

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_compile_program(

```
....
492.                 "#define FRAGMENT\n#define PARAMETER_UNIFORM\n",
```

File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_compile_shader(glsl_shader_data_t *glsl,

```
....
405.     source[1] = define;
```

Buffer Overflow LongString\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=3
Status New

The size of the buffer used by gl_glsl_compile_shader in source, at line 349 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_compile_program passes to "#define VERTEX\n#define PARAMETER_UNIFORM\n", at line 453 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	478	405
Object	"#define VERTEX\n#define PARAMETER_UNIFORM\n"	source

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_compile_program(

```
....
478.                  "#define VERTEX\n#define PARAMETER_UNIFORM\n",
program_info->vertex))
```

File Name RetroArch/shader_glsl.c

Method static bool gl_glsl_compile_shader(glsl_shader_data_t *glsl,

```
....
405.     source[1] = define;
```

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=1010010&projectid=10011&pathid=13
Status	New

The size of the buffer used by load_wavefront_obj in material, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to name, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	247	250
Object	name	material

Code Snippet

File Name RetroArch/models.c

Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
247.           if (sscanf(s, "usemtl %s", /*MAX_MATERIAL_NAME-1,
*/model->material[m->num_materials].name) == 1) {
....
250.                    strcpy(model->material[m->num_materials-1].name,
model->material[m->num_materials].name);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=14
Status	New

The size of the buffer used by load_wavefront_obj in material, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to name, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	247	250
Object	name	material

Code Snippet

File Name RetroArch/models.c

Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
247.            if (sscanf(s, "usemtl %s", /*MAX_MATERIAL_NAME-1,
*/model->material[m->num_materials].name) == 1) {
....
250.                    strcpy(model->material[m->num_materials-1].name,
model->material[m->num_materials].name);
```

Buffer Overflow boundedcpy

Query Path:

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

Categories

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

Description

Buffer Overflow boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=4
Status	New

The size parameter len in line 1985 in file RetroArch/test_x509.c is influenced by the user input argv in line 1985 in file RetroArch/test_x509.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination

File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1985	2014
Object	argv	len

Code Snippet
File Name RetroArch/test_x509.c
Method main(int argc, const char *argv[])

```
....
1985.  main(int argc, const char *argv[])
....
2014.                          memcpy(dn, arg, len);
```

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=1010010&projectid=10011&pathid=625
Status New

The dangerous function, memcpy, was found in use at line 876 in RetroArch/btstack_hid.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	886	886
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_queue_hci_remote_name_request(

```
....
886.     memcpy(cmd->hci_remote_name_request.bd_addr, bd_addr,
sizeof(bd_addr_t));
```

Dangerous Functions\Path 2:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=626
Status	New

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

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	904	904
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_queue_hci_pin_code_request_reply(

```
....
904.     memcpy(cmd->hci_pin_code_request_reply.bd_addr, bd_addr,
sizeof(bd_addr_t));
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=627
Status	New

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

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	905	905
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_queue_hci_pin_code_request_reply(

```
....
905.     memcpy(cmd->hci_pin_code_request_reply.pin, pin,
sizeof(bd_addr_t));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=100

	11&pathid=628
Status	New

The dangerous function, memcpy, was found in use at line 1003 in RetroArch/btstack_hid.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	1086	1086
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_packet_handler(uint8_t packet_type,

```
....
1086.                    memcpy(connection->address, event_addr,
sizeof(bd_addr_t));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=629
Status	New

The dangerous function, memcpy, was found in use at line 1003 in RetroArch/btstack_hid.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	1175	1175
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_packet_handler(uint8_t packet_type,

```
....
1175.                        memcpy(connection->address, event_addr,
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=630
Status	New

The dangerous function, memcpy, was found in use at line 260 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	305	305
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_send_command_win32(const libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, unsigned char *sense, size_t sense_len)

```
....
305.     memcpy(sptd.s.Cdb, cmd, cmd_len);
```

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=631
Status New

The dangerous function, memcpy, was found in use at line 374 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	457	457
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
457.             memcpy(xfer_buf_pos, stream->cdrom.last_frame,
sizeof(stream->cdrom.last_frame));
```

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=100

	11&pathid=632
Status	New

The dangerous function, memcpy, was found in use at line 374 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	500	500
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
500.                memcpy((char*)buf + copied_bytes, xfer_buf_pos + skip,
copy_len);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=633
Status	New

The dangerous function, memcpy, was found in use at line 374 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	508	508
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
508.                    memcpy(stream->cdrom.last_frame, xfer_buf_pos,
sizeof(stream->cdrom.last_frame));
```

Dangerous Functions\Path 10:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=634
Status	New

The dangerous function, memcpy, was found in use at line 968 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	985	985
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_read_track_info(libretro_vfs_implementation_file *stream, unsigned char track, cdrom_toc_t *toc)

```
....
985.     memcpy(&lba, buf + 8, 4);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=635
Status	New

The dangerous function, memcpy, was found in use at line 968 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	986	986
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_read_track_info(libretro_vfs_implementation_file *stream, unsigned char track, cdrom_toc_t *toc)

```
....
986.     memcpy(&track_size, buf + 24, 4);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=636
Status	New

The dangerous function, memcpy, was found in use at line 1161 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1177	1177
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method int cdrom_get_inquiry(libretro_vfs_implementation_file *stream, char *model, int len, bool *is_cdrom)

```
....
1177.         memcpy(model, buf + 8, 8);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=637
Status	New

The dangerous function, memcpy, was found in use at line 1161 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1182	1182
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method int cdrom_get_inquiry(libretro_vfs_implementation_file *stream, char *model, int len, bool *is_cdrom)

```
....
1182.         memcpy(model + 9, buf + 16, 16);
```

Dangerous Functions\Path 14:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=638
Status	New

The dangerous function, memcpy, was found in use at line 1161 in RetroArch/cdrom.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1187	1187
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/cdrom.c
Method int cdrom_get_inquiry(libretro_vfs_implementation_file *stream, char *model, int len, bool *is_cdrom)

```
....
1187.         memcpy(model + 26, buf + 32, 4);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=639
Status	New

The dangerous function, memcpy, was found in use at line 309 in RetroArch/drm_gfx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	321	321
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_surface_update(void *data, const void *frame,

```
....
321.         memcpy (
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=640

Status	New

The dangerous function, memcpy, was found in use at line 808 in RetroArch/drm_gfx.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	863	863
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_set_texture_frame(void *data, const void *frame, bool rgb32,

```
....
863.        memcpy(dst_base_addr + (dst_pitch * i), (char*)line,
dst_pitch);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=641
Status	New

The dangerous function, memcpy, was found in use at line 364 in RetroArch/dtoverlay_main.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	379	379
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method int dtparam_apply(DTBLOB_T *dtb, const char *override_name,

```
....
379.        memcpy(data, override_data, data_len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=642
Status	New

The dangerous function, memcpy, was found in use at line 111 in RetroArch/hbl.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c
Line	144	144
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/hbl.c
Method static int HomebrewCopyMemory(u8 *address, u32 bytes, u32 args_size)

```
....
144.        memcpy((void *)ELF_DATA_ADDR, address, bytes);
```

Dangerous Functions\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=643
Status New

The dangerous function, memcpy, was found in use at line 487 in RetroArch/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	491	491
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
491.        memcpy(out, source + 1, l * sizeof(char));
```

Dangerous Functions\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=644
Status New

The dangerous function, memcpy, was found in use at line 487 in RetroArch/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	499	499
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
499.        memcpy(out, source + 1, l * sizeof(char));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=645
Status	New

The dangerous function, memcpy, was found in use at line 487 in RetroArch/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	503	503
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
503.        memcpy(out, source + 1 + l - bufflen, bufflen *
sizeof(char));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=646
Status	New

The dangerous function, memcpy, was found in use at line 487 in RetroArch/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	RetroArch/lobject.c	RetroArch/lobject.c
Line	519	519
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
519.      memcpy(out, POS, (LL(POS) + 1) * sizeof(char));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=647
Status	New

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

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	135	135
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
135.        memcpy(p, s, l * sizeof(char)); p += l;
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=648
Status	New

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

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	137	137

Object	memcpy	memcpy

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
137.          memcpy(p, sep, lsep * sizeof(char));
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=649
Status	New

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

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	141	141
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
141.      memcpy(p, s, l * sizeof(char));  /* last copy (not followed by
separator) */
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=650
Status	New

The dangerous function, memcpy, was found in use at line 981 in RetroArch/lstrlib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	996	996
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/lstrlib.c
Method	static const char *scanformat (lua_State *L, const char *strfrmt, char *form) {

```
....
996.    memcpy(form, strfrmt, ((p - strfrmt) + 1) * sizeof(char));
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=651
Status	New

The dangerous function, memcpy, was found in use at line 460 in RetroArch/lvm.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/lvm.c	RetroArch/lvm.c
Line	464	464
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/lvm.c
Method	static void copy2buff (StkId top, int n, char *buff) {

```
....
464.      memcpy(buff + tl, svalue(top - n), l * sizeof(char));
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=652
Status	New

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

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	335	335
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/models.c

Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=653
Status	New

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

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	336	336
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=654
Status	New

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

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	337	337
Object	memcpy	memcpy

Code Snippet

File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
337.     memcpy((float *)m->data + m->numv + m->numt + m->numn, (float
*)m->data + (3 + 2 + 3) * MAX_VERTICES, m->numf * sizeof *qf);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=655
Status	New

The dangerous function, memcpy, was found in use at line 586 in RetroArch/net_http.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	638	638
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/net_http.c
Method	bool net_http_connection_done(struct http_connection_t *conn)

```
....
638.           memcpy(urlcopy, conn->domain, domain_len);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=656
Status	New

The dangerous function, memcpy, was found in use at line 586 in RetroArch/net_http.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	640	640
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/net_http.c

Method	bool net_http_connection_done(struct http_connection_t *conn)

```
....
640.            memcpy(urlcopy + domain_len + 1, conn->scan, location_len
+ 1);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=657
Status	New

The dangerous function, memcpy, was found in use at line 235 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	267	267
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c
Method	int rc_json_parse_response(rc_api_response_t* response, const char* json, rc_json_field_t* fields, size_t field_count) {

```
....
267.        memcpy(dst, json, end - json);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=658
Status	New

The dangerous function, memcpy, was found in use at line 278 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	286	286
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c

Method	static int rc_json_missing_field(rc_api_response_t* response, const rc_json_field_t* field) {

```
....
286.      memcpy(write, field->name, field_len);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=659
Status	New

The dangerous function, memcpy, was found in use at line 278 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	288	288
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c
Method	static int rc_json_missing_field(rc_api_response_t* response, const rc_json_field_t* field) {

```
....
288.      memcpy(write, not_found, not_found_len + 1);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=660
Status	New

The dangerous function, memcpy, was found in use at line 360 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	373	373
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c

Method	int rc_json_get_required_array(unsigned* num_entries, rc_json_field_t* iterator, rc_api_response_t* response, const rc_json_field_t* field, const char* field_name) {

```
....
373.    memcpy(iterator, field, sizeof(*iterator));
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=661
Status	New

The dangerous function, memcpy, was found in use at line 398 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	401	401
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c
Method	static unsigned rc_json_decode_hex4(const char* input) {

```
....
401.    memcpy(hex, input, 4);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=662
Status	New

The dangerous function, memcpy, was found in use at line 452 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	544	544
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c

Method	int rc_json_get_string(const char** out, rc_api_buffer_t* buffer, const rc_json_field_t* field, const char* field_name) {

```
....
544.      memcpy(dst, src, len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=663
Status	New

The dangerous function, memcpy, was found in use at line 876 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	904	904
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c
Method	static int rc_url_builder_reserve(rc_api_url_builder_t* builder, size_t amount) {

```
....
904.          memcpy(new_start, builder->start, used);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=664
Status	New

The dangerous function, memcpy, was found in use at line 916 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	945	945
Object	memcpy	memcpy

Code Snippet	
File Name	RetroArch/rc_api_common.c
Method	void rc_url_builder_append_encoded_str(rc_api_url_builder_t* builder, const char* str) {

```
....
945.            memcpy(builder->write, start, len);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=665
Status	New

The dangerous function, memcpy, was found in use at line 964 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	966	966
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rc_api_common.c
Method void rc_url_builder_append(rc_api_url_builder_t* builder, const char* data, size_t len) {

```
....
966.      memcpy(builder->write, data, len);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=666
Status	New

The dangerous function, memcpy, was found in use at line 971 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	980	980
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rc_api_common.c
Method static int rc_url_builder_append_param_equals(rc_api_url_builder_t* builder, const char* param) {

```
....
980.      memcpy(builder->write, param, param_len);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=667
Status	New

The dangerous function, memcpy, was found in use at line 1009 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	1022	1022
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rc_api_common.c
Method void rc_api_url_build_dorequest_url(rc_api_request_t* request) {

```
....
1022.      memcpy(url, g_host, host_len);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=668
Status	New

The dangerous function, memcpy, was found in use at line 1009 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	1023	1023
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rc_api_common.c
Method void rc_api_url_build_dorequest_url(rc_api_request_t* request) {

```
....
1023.      memcpy(url + host_len, DOREQUEST_ENDPOINT, endpoint_len);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=669
Status	New

The dangerous function, memcpy, was found in use at line 1046 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	1062	1062
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rc_api_common.c
Method static void rc_api_update_host(char** host, const char* hostname) {

```
....
1062.            memcpy(newhost, "http://", 7);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=670
Status	New

The dangerous function, memcpy, was found in use at line 1046 in RetroArch/rc_api_common.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	1063	1063
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rc_api_common.c
Method static void rc_api_update_host(char** host, const char* hostname) {

```
....
1063.            memcpy(&newhost[7], hostname, hostname_len + 1);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=671
Status	New

The dangerous function, memcpy, was found in use at line 1629 in RetroArch/rgui.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	1673	1673
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_fill_rect(

```
....
1673.            memcpy(dst + (y_index * fb_width), src, x_size);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=672
Status	New

The dangerous function, memcpy, was found in use at line 1629 in RetroArch/rgui.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	1724	1724
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_fill_rect(

```
....
1724.           memcpy(dst + (y_index * fb_width), src_a, x_size);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=673
Status	New

The dangerous function, memcpy, was found in use at line 1629 in RetroArch/rgui.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	1727	1727
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_fill_rect(

```
....
1727.           memcpy(dst + (y_index * fb_width), src_b, x_size);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=674
Status	New

The dangerous function, memcpy, was found in use at line 1629 in RetroArch/rgui.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	1730	1730
Object	memcpy	memcpy

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_fill_rect(

```
....
1730.           memcpy(dst + (y_index * fb_width), src_c, x_size);
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1000
Status	New

	Source	Destination
File	RetroArch/CpuArch.c	RetroArch/CpuArch.c
Line	64	75
Object	a2	a2

Code Snippet
File Name RetroArch/CpuArch.c
Method void MyCPUID(uint32_t function, uint32_t *a, uint32_t *b, uint32_t *c, uint32_t *d)

```
....
64.    uint32_t a2, b2, c2, d2;
....
75.    *a = a2;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1001
Status	New

	Source	Destination
File	RetroArch/CpuArch.c	RetroArch/CpuArch.c
Line	64	76
Object	b2	b2

Code Snippet

File Name	RetroArch/CpuArch.c
Method	void MyCPUID(uint32_t function, uint32_t *a, uint32_t *b, uint32_t *c, uint32_t *d)

```
....
64.    uint32_t a2, b2, c2, d2;
....
76.    *b = b2;
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1002
Status	New

	Source	Destination
File	RetroArch/CpuArch.c	RetroArch/CpuArch.c
Line	64	77
Object	c2	c2

Code Snippet

File Name	RetroArch/CpuArch.c
Method	void MyCPUID(uint32_t function, uint32_t *a, uint32_t *b, uint32_t *c, uint32_t *d)

```
....
64.    uint32_t a2, b2, c2, d2;
....
77.    *c = c2;
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1003
Status	New

	Source	Destination
File	RetroArch/CpuArch.c	RetroArch/CpuArch.c
Line	64	78
Object	d2	d2

Code Snippet

File Name	RetroArch/CpuArch.c
Method	void MyCPUID(uint32_t function, uint32_t *a, uint32_t *b, uint32_t *c, uint32_t *d)

```
....
64.    uint32_t a2, b2, c2, d2;
....
78.    *d = d2;
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1004
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	103	224
Object	_9_10_weight_1_3	_9_10_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
103.           uint16_t  _9_10_weight_1_3;
....
224.           UPSCALE_256__WEIGHT_1_3(_9_10_weight_1_3,
_13_14_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1005
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	103	224
Object	_9_10_weight_1_3	_9_10_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
103.            uint16_t  _9_10_weight_1_3;
....
224.            UPSCALE_256__WEIGHT_1_3(_9_10_weight_1_3,
_13_14_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1006
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	103	207
Object	_9_10_weight_1_3	_9_10_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
103.            uint16_t  _9_10_weight_1_3;
....
207.            *(block_dst_ptr + 1) = _9_10_weight_1_3;
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1007
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	104	229
Object	_11_12_weight_3_1	_11_12_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
104.            uint16_t _11_12_weight_3_1;
....
229.            UPSCALE_256__WEIGHT_1_3(_11_12_weight_3_1,
_15_16_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1008
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	104	229
Object	_11_12_weight_3_1	_11_12_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
104.            uint16_t _11_12_weight_3_1;
....
229.            UPSCALE_256__WEIGHT_1_3(_11_12_weight_3_1,
_15_16_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1009
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	104	210
Object	_11_12_weight_3_1	_11_12_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
104.            uint16_t _11_12_weight_3_1;
....
210.            *(block_dst_ptr + 3) = _11_12_weight_3_1;
```

Use of Uninitialized Variable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1010
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	105	243
Object	_13_14_weight_1_3	_13_14_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
105.            uint16_t _13_14_weight_1_3;
....
243.            UPSCALE_256__WEIGHT_1_3(_13_14_weight_1_3,
_17_18_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1011
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	105	243
Object	_13_14_weight_1_3	_13_14_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
105.            uint16_t _13_14_weight_1_3;
....
243.            UPSCALE_256__WEIGHT_1_3(_13_14_weight_1_3,
_17_18_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1012
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	105	224
Object	_13_14_weight_1_3	_13_14_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
105.            uint16_t _13_14_weight_1_3;
....
224.            UPSCALE_256__WEIGHT_1_3(_9_10_weight_1_3,
_13_14_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1013
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	105	224
Object	_13_14_weight_1_3	_13_14_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
105.            uint16_t _13_14_weight_1_3;
....
224.            UPSCALE_256__WEIGHT_1_3(_9_10_weight_1_3,
_13_14_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1014
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	105	224
Object	_13_14_weight_1_3	_13_14_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
105.            uint16_t _13_14_weight_1_3;
....
224.            UPSCALE_256__WEIGHT_1_3(_9_10_weight_1_3,
_13_14_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1015
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	105	224
Object	_13_14_weight_1_3	_13_14_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
105.            uint16_t _13_14_weight_1_3;
....
224.            UPSCALE_256__WEIGHT_1_3(_9_10_weight_1_3,
_13_14_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1016
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	106	227
Object	_10_11_weight_1_1	_10_11_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
106.            uint16_t _10_11_weight_1_1;
....
227.            UPSCALE_256__WEIGHT_1_3(_10_11_weight_1_1,
_14_15_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1017
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	106	227
Object	_10_11_weight_1_1	_10_11_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
106.            uint16_t _10_11_weight_1_1;
....
227.            UPSCALE_256__WEIGHT_1_3(_10_11_weight_1_1,
_14_15_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1018
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	107	245
Object	_14_15_weight_1_1	_14_15_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
107.            uint16_t _14_15_weight_1_1;
....
245.            UPSCALE_256__WEIGHT_1_3(_14_15_weight_1_1,
_18_19_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1019
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	107	245
Object	_14_15_weight_1_1	_14_15_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
107.            uint16_t _14_15_weight_1_1;
....
245.            UPSCALE_256__WEIGHT_1_3(_14_15_weight_1_1,
_18_19_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1020
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	107	227
Object	_14_15_weight_1_1	_14_15_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
107.            uint16_t _14_15_weight_1_1;
....
227.            UPSCALE_256__WEIGHT_1_3(_10_11_weight_1_1,
_14_15_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1021
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	107	227
Object	_14_15_weight_1_1	_14_15_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
107.            uint16_t _14_15_weight_1_1;
....
227.            UPSCALE_256__WEIGHT_1_3(_10_11_weight_1_1,
_14_15_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1022
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	107	227
Object	_14_15_weight_1_1	_14_15_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
107.            uint16_t _14_15_weight_1_1;
....
227.            UPSCALE_256__WEIGHT_1_3(_10_11_weight_1_1,
_14_15_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1023
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	107	227
Object	_14_15_weight_1_1	_14_15_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
107.            uint16_t _14_15_weight_1_1;
....
227.            UPSCALE_256__WEIGHT_1_3(_10_11_weight_1_1,
_14_15_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1024
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	108	247
Object	_15_16_weight_3_1	_15_16_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
108.            uint16_t _15_16_weight_3_1;
....
247.            UPSCALE_256__WEIGHT_1_3(_15_16_weight_3_1,
_19_20_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1025
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	108	247
Object	_15_16_weight_3_1	_15_16_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
108.            uint16_t _15_16_weight_3_1;
....
247.            UPSCALE_256__WEIGHT_1_3(_15_16_weight_3_1,
_19_20_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1026
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	108	229
Object	_15_16_weight_3_1	_15_16_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
108.            uint16_t _15_16_weight_3_1;
....
229.            UPSCALE_256__WEIGHT_1_3(_11_12_weight_3_1,
_15_16_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1027
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	108	229
Object	_15_16_weight_3_1	_15_16_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
108.            uint16_t _15_16_weight_3_1;
....
229.            UPSCALE_256__WEIGHT_1_3(_11_12_weight_3_1,
_15_16_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1028
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	108	229
Object	_15_16_weight_3_1	_15_16_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
108.            uint16_t _15_16_weight_3_1;
....
229.            UPSCALE_256__WEIGHT_1_3(_11_12_weight_3_1,
_15_16_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1029
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	108	229
Object	_15_16_weight_3_1	_15_16_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
108.            uint16_t _15_16_weight_3_1;
....
229.            UPSCALE_256__WEIGHT_1_3(_11_12_weight_3_1,
_15_16_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1030
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	109	261
Object	_17_18_weight_1_3	_17_18_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
109.            uint16_t _17_18_weight_1_3;
....
261.            UPSCALE_256__WEIGHT_1_3(_17_18_weight_1_3,
_21_22_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1031
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	109	261
Object	_17_18_weight_1_3	_17_18_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
109.            uint16_t _17_18_weight_1_3;
....
261.            UPSCALE_256__WEIGHT_1_3(_17_18_weight_1_3,
_21_22_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1032
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	109	243
Object	_17_18_weight_1_3	_17_18_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
109.            uint16_t _17_18_weight_1_3;
....
243.            UPSCALE_256__WEIGHT_1_3(_13_14_weight_1_3,
_17_18_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1033
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	109	243
Object	_17_18_weight_1_3	_17_18_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
109.            uint16_t _17_18_weight_1_3;
....
243.            UPSCALE_256__WEIGHT_1_3(_13_14_weight_1_3,
_17_18_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1034
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	109	243
Object	_17_18_weight_1_3	_17_18_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
109.            uint16_t _17_18_weight_1_3;
....
243.            UPSCALE_256__WEIGHT_1_3(_13_14_weight_1_3,
_17_18_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1035
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	109	243
Object	_17_18_weight_1_3	_17_18_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
109.            uint16_t _17_18_weight_1_3;
....
243.            UPSCALE_256__WEIGHT_1_3(_13_14_weight_1_3,
_17_18_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1036
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	110	263
Object	_18_19_weight_1_1	_18_19_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
110.            uint16_t _18_19_weight_1_1;
....
263.            UPSCALE_256__WEIGHT_1_3(_18_19_weight_1_1,
_22_23_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1037
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	110	263
Object	_18_19_weight_1_1	_18_19_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
110.            uint16_t _18_19_weight_1_1;
....
263.            UPSCALE_256__WEIGHT_1_3(_18_19_weight_1_1,
_22_23_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1038
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	110	245
Object	_18_19_weight_1_1	_18_19_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
110.            uint16_t _18_19_weight_1_1;
....
245.            UPSCALE_256__WEIGHT_1_3(_14_15_weight_1_1,
_18_19_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1039
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	110	245
Object	_18_19_weight_1_1	_18_19_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
110.            uint16_t _18_19_weight_1_1;
....
245.            UPSCALE_256__WEIGHT_1_3(_14_15_weight_1_1,
_18_19_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1040
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	110	245
Object	_18_19_weight_1_1	_18_19_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
110.            uint16_t _18_19_weight_1_1;
....
245.            UPSCALE_256__WEIGHT_1_3(_14_15_weight_1_1,
_18_19_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1041
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	110	245
Object	_18_19_weight_1_1	_18_19_weight_1_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
110.            uint16_t _18_19_weight_1_1;
....
245.            UPSCALE_256__WEIGHT_1_3(_14_15_weight_1_1,
_18_19_weight_1_1, block_dst_ptr + 2, tmp);
```

Use of Uninitialized Variable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1042
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	111	265
Object	_19_20_weight_3_1	_19_20_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
111.            uint16_t _19_20_weight_3_1;
....
265.            UPSCALE_256__WEIGHT_1_3(_19_20_weight_3_1,
_23_24_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1043
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	111	265
Object	_19_20_weight_3_1	_19_20_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
111.            uint16_t _19_20_weight_3_1;
....
265.            UPSCALE_256__WEIGHT_1_3(_19_20_weight_3_1,
_23_24_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1044
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	111	247
Object	_19_20_weight_3_1	_19_20_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
111.            uint16_t _19_20_weight_3_1;
....
247.            UPSCALE_256__WEIGHT_1_3(_15_16_weight_3_1,
_19_20_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1045
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	111	247
Object	_19_20_weight_3_1	_19_20_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
111.            uint16_t _19_20_weight_3_1;
....
247.            UPSCALE_256__WEIGHT_1_3(_15_16_weight_3_1,
_19_20_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1046
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	111	247
Object	_19_20_weight_3_1	_19_20_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
111.            uint16_t _19_20_weight_3_1;
....
247.            UPSCALE_256__WEIGHT_1_3(_15_16_weight_3_1,
_19_20_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1047
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	111	247
Object	_19_20_weight_3_1	_19_20_weight_3_1

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
111.            uint16_t _19_20_weight_3_1;
....
247.            UPSCALE_256__WEIGHT_1_3(_15_16_weight_3_1,
_19_20_weight_3_1, block_dst_ptr + 3, tmp);
```

Use of Uninitialized Variable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1048
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	112	279
Object	_21_22_weight_1_3	_21_22_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
112.            uint16_t _21_22_weight_1_3;
....
279.            UPSCALE_256__WEIGHT_1_3(_21_22_weight_1_3,
_25_26_weight_1_3, block_dst_ptr + 1, tmp);
```

Use of Uninitialized Variable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1049
Status	New

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	112	279
Object	_21_22_weight_1_3	_21_22_weight_1_3

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method void upscale_256x224_to_320x240(uint16_t *dst, const uint16_t *src,

```
....
112.            uint16_t _21_22_weight_1_3;
....
279.            UPSCALE_256__WEIGHT_1_3(_21_22_weight_1_3,
_25_26_weight_1_3, block_dst_ptr + 1, tmp);
```

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=1010010&projectid=10011&pathid=17
Status	New

The size of the buffer used by btpad_queue_hci_remote_name_request in bd_addr_t, at line 876 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that btpad_queue_hci_remote_name_request passes to bd_addr_t, at line 876 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	886	886
Object	bd_addr_t	bd_addr_t

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_queue_hci_remote_name_request(

```
....
886.     memcpy(cmd->hci_remote_name_request.bd_addr, bd_addr,
sizeof(bd_addr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=18
Status	New

The size of the buffer used by btpad_queue_hci_pin_code_request_reply in bd_addr_t, at line 896 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that btpad_queue_hci_pin_code_request_reply passes to bd_addr_t, at line 896 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	904	904
Object	bd_addr_t	bd_addr_t

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_queue_hci_pin_code_request_reply(

```
....
904.     memcpy(cmd->hci_pin_code_request_reply.bd_addr, bd_addr,
sizeof(bd_addr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=19
Status New

The size of the buffer used by btpad_queue_hci_pin_code_request_reply in bd_addr_t, at line 896 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that btpad_queue_hci_pin_code_request_reply passes to bd_addr_t, at line 896 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	905	905
Object	bd_addr_t	bd_addr_t

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_queue_hci_pin_code_request_reply(

```
....
905.     memcpy(cmd->hci_pin_code_request_reply.pin, pin,
sizeof(bd_addr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=20
Status New

The size of the buffer used by btpad_packet_handler in bd_addr_t, at line 1003 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that btpad_packet_handler passes to bd_addr_t, at line 1003 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	1086	1086
Object	bd_addr_t	bd_addr_t

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_packet_handler(uint8_t packet_type,

```
....
1086.                    memcpy(connection->address, event_addr,
sizeof(bd_addr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=21
Status New

The size of the buffer used by btpad_packet_handler in bd_addr_t, at line 1003 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that btpad_packet_handler passes to bd_addr_t, at line 1003 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	1176	1176
Object	bd_addr_t	bd_addr_t

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_packet_handler(uint8_t packet_type,

```
....
1176.                              sizeof(bd_addr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=22
Status New

The size of the buffer used by cdrom_send_command in Namespace535592194, at line 374 of RetroArch/cdrom.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cdrom_send_command passes to Namespace535592194, at line 374 of RetroArch/cdrom.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	457	457
Object	Namespace535592194	Namespace535592194

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
457.              memcpy(xfer_buf_pos, stream->cdrom.last_frame,
sizeof(stream->cdrom.last_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=23
Status New

The size of the buffer used by cdrom_send_command in Namespace535592194, at line 374 of RetroArch/cdrom.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cdrom_send_command passes to Namespace535592194, at line 374 of RetroArch/cdrom.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	508	508
Object	Namespace535592194	Namespace535592194

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
508.                  memcpy(stream->cdrom.last_frame, xfer_buf_pos,
sizeof(stream->cdrom.last_frame));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium
Result State To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=24
Status	New

The size of the buffer used by rgui_blit_line_regular_shadow in color_buf, at line 3394 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_regular_shadow passes to color_buf, at line 3394 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3437	3437
Object	color_buf	color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_regular_shadow(

```
....
3437.                     memcpy(frame_buf_ptr, color_buf,
sizeof(color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=25
Status	New

The size of the buffer used by rgui_blit_line_regular_shadow in shadow_color_buf, at line 3394 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_regular_shadow passes to shadow_color_buf, at line 3394 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3441	3441
Object	shadow_color_buf	shadow_color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_regular_shadow(

```
....
3441.                     memcpy(frame_buf_ptr, shadow_color_buf,
sizeof(shadow_color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=26
Status	New

The size of the buffer used by rgui_blit_line_extended_shadow in color_buf, at line 3505 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_extended_shadow passes to color_buf, at line 3505 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3562	3562
Object	color_buf	color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_extended_shadow(

```
....
3562.                    memcpy(frame_buf_ptr, color_buf,
sizeof(color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=27
Status	New

The size of the buffer used by rgui_blit_line_extended_shadow in shadow_color_buf, at line 3505 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_extended_shadow passes to shadow_color_buf, at line 3505 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3566	3566
Object	shadow_color_buf	shadow_color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_extended_shadow(

```
....
3566.                    memcpy(frame_buf_ptr, shadow_color_buf,
sizeof(shadow_color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=28
Status	New

The size of the buffer used by rgui_blit_line_cjk_shadow in color_buf, at line 3637 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_cjk_shadow passes to color_buf, at line 3637 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3700	3700
Object	color_buf	color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_cjk_shadow(

```
....
3700.                    memcpy(frame_buf_ptr, color_buf,
sizeof(color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=29
Status	New

The size of the buffer used by rgui_blit_line_cjk_shadow in shadow_color_buf, at line 3637 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_cjk_shadow passes to shadow_color_buf, at line 3637 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3704	3704
Object	shadow_color_buf	shadow_color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_cjk_shadow(

```
....
3704.                    memcpy(frame_buf_ptr, shadow_color_buf,
sizeof(shadow_color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=30
Status	New

The size of the buffer used by rgui_blit_line_rus_shadow in color_buf, at line 3768 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_rus_shadow passes to color_buf, at line 3768 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3825	3825
Object	color_buf	color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_rus_shadow(

```
....
3825.                    memcpy(frame_buf_ptr, color_buf,
sizeof(color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=31
Status	New

The size of the buffer used by rgui_blit_line_rus_shadow in shadow_color_buf, at line 3768 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_rus_shadow passes to shadow_color_buf, at line 3768 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3829	3829
Object	shadow_color_buf	shadow_color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_rus_shadow(

```
....
3829.                    memcpy(frame_buf_ptr, shadow_color_buf,
sizeof(shadow_color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=32
Status	New

The size of the buffer used by rgui_blit_line_6x10_shadow in color_buf, at line 3887 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_6x10_shadow passes to color_buf, at line 3887 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3938	3938
Object	color_buf	color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_6x10_shadow(

```
....
3938.                    memcpy(frame_buf_ptr, color_buf,
sizeof(color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=33
Status	New

The size of the buffer used by rgui_blit_line_6x10_shadow in shadow_color_buf, at line 3887 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_line_6x10_shadow passes to shadow_color_buf, at line 3887 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3942	3942
Object	shadow_color_buf	shadow_color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_line_6x10_shadow(

```
....
3942.                    memcpy(frame_buf_ptr, shadow_color_buf,
sizeof(shadow_color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=34
Status	New

The size of the buffer used by rgui_blit_symbol_shadow in color_buf, at line 4274 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_symbol_shadow passes to color_buf, at line 4274 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	4309	4309
Object	color_buf	color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_symbol_shadow(

```
....
4309.              memcpy(frame_buf_ptr, color_buf, sizeof(color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=35
Status	New

The size of the buffer used by rgui_blit_symbol_shadow in shadow_color_buf, at line 4274 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rgui_blit_symbol_shadow passes to shadow_color_buf, at line 4274 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	4313	4313
Object	shadow_color_buf	shadow_color_buf

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_blit_symbol_shadow(

```
....
4313.              memcpy(frame_buf_ptr, shadow_color_buf,
sizeof(shadow_color_buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=36
Status	New

The size of the buffer used by ssl_srv_parse_session_ticket_ext in mbedtls_ssl_session, at line 436 of RetroArch/ssl_srv.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssl_srv_parse_session_ticket_ext passes to mbedtls_ssl_session, at line 436 of RetroArch/ssl_srv.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	493	493
Object	mbedtls_ssl_session	mbedtls_ssl_session

Code Snippet
File Name RetroArch/ssl_srv.c
Method static int ssl_srv_parse_session_ticket_ext(mbedtls_ssl_context *ssl,

```
....
493.      memcpy( ssl->session_negotiate, &session, sizeof(
mbedtls_ssl_session ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=37
Status	New

The size of the buffer used by xmb_draw_fullscreen_thumbnails in mean_menu_color, at line 5194 of RetroArch/xmb.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmb_draw_fullscreen_thumbnails passes to mean_menu_color, at line 5194 of RetroArch/xmb.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5440	5440
Object	mean_menu_color	mean_menu_color

Code Snippet
File Name RetroArch/xmb.c

Method	static void xmb_draw_fullscreen_thumbnails(

```
....
5440.           memcpy(frame_color,      mean_menu_color,
sizeof(mean_menu_color));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=38
Status	New

The size of the buffer used by xmb_draw_fullscreen_thumbnails in mean_menu_color, at line 5194 of RetroArch/xmb.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmb_draw_fullscreen_thumbnails passes to mean_menu_color, at line 5194 of RetroArch/xmb.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5441	5441
Object	mean_menu_color	mean_menu_color

Code Snippet	
File Name	RetroArch/xmb.c
Method	static void xmb_draw_fullscreen_thumbnails(

```
....
5441.           memcpy(frame_color + 4,  mean_menu_color,
sizeof(mean_menu_color));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=39
Status	New

The size of the buffer used by xmb_draw_fullscreen_thumbnails in mean_menu_color, at line 5194 of RetroArch/xmb.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmb_draw_fullscreen_thumbnails passes to mean_menu_color, at line 5194 of RetroArch/xmb.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5442	5442
Object	mean_menu_color	mean_menu_color

Code Snippet

File Name	RetroArch/xmb.c
Method	static void xmb_draw_fullscreen_thumbnails(

```
....
5442.           memcpy(frame_color + 8,  mean_menu_color,
sizeof(mean_menu_color));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=40
Status	New

The size of the buffer used by xmb_draw_fullscreen_thumbnails in mean_menu_color, at line 5194 of RetroArch/xmb.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmb_draw_fullscreen_thumbnails passes to mean_menu_color, at line 5194 of RetroArch/xmb.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5443	5443
Object	mean_menu_color	mean_menu_color

Code Snippet	
File Name	RetroArch/xmb.c
Method	static void xmb_draw_fullscreen_thumbnails(

```
....
5443.           memcpy(frame_color + 12, mean_menu_color,
sizeof(mean_menu_color));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=41
Status	New

The size of the buffer used by xmb_list_deep_copy in menu_file_list_cbs_t, at line 7522 of RetroArch/xmb.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmb_list_deep_copy passes to menu_file_list_cbs_t, at line 7522 of RetroArch/xmb.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7554	7554
Object	menu_file_list_cbs_t	menu_file_list_cbs_t

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_list_deep_copy(const file_list_t *src, file_list_t *dst,

```
....
7554.           memcpy(data, src_adata, sizeof(menu_file_list_cbs_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=42
Status New

The size of the buffer used by btpad_close_connection in btstack_hid_adapter, at line 911 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that btpad_close_connection passes to btstack_hid_adapter, at line 911 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	920	920
Object	btstack_hid_adapter	btstack_hid_adapter

Code Snippet
File Name RetroArch/btstack_hid.c
Method static void btpad_close_connection(struct btstack_hid_adapter* connection)

```
....
920.     memset(connection, 0, sizeof(struct btstack_hid_adapter));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=43
Status New

The size of the buffer used by btpad_packet_handler in btstack_hid_adapter, at line 1003 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that btpad_packet_handler passes to btstack_hid_adapter, at line 1003 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	1084	1084
Object	btstack_hid_adapter	btstack_hid_adapter

Code Snippet

File Name	RetroArch/btstack_hid.c
Method	static void btpad_packet_handler(uint8_t packet_type,

```
....
1084.                    memset(connection, 0, sizeof(struct
btstack_hid_adapter));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=44
Status	New

The size of the buffer used by btpad_packet_handler in btstack_hid_adapter, at line 1003 of RetroArch/btstack_hid.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that btpad_packet_handler passes to btstack_hid_adapter, at line 1003 of RetroArch/btstack_hid.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	1173	1173
Object	btstack_hid_adapter	btstack_hid_adapter

Code Snippet

File Name	RetroArch/btstack_hid.c
Method	static void btpad_packet_handler(uint8_t packet_type,

```
....
1173.                            sizeof(struct btstack_hid_adapter));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=45
Status	New

The size of the buffer used by retroarch_deinit_drivers in turbo_buttons_t, at line 1156 of RetroArch/retroarch.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that retroarch_deinit_drivers passes to turbo_buttons_t, at line 1156 of RetroArch/retroarch.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	1207	1207
Object	turbo_buttons_t	turbo_buttons_t

Code Snippet

File Name	RetroArch/retroarch.c
Method	static void retroarch_deinit_drivers(struct retro_callbacks *cbs)

```
....
1207.        memset(&input_st->turbo_btns, 0, sizeof(turbo_buttons_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=46
Status	New

The size of the buffer used by retroarch_deinit_drivers in ->, at line 1156 of RetroArch/retroarch.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that retroarch_deinit_drivers passes to ->, at line 1156 of RetroArch/retroarch.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	1209	1209
Object	->	->

Code Snippet	
File Name	RetroArch/retroarch.c
Method	static void retroarch_deinit_drivers(struct retro_callbacks *cbs)

```
....
1209.            sizeof(input_st->analog_requested));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=47
Status	New

The size of the buffer used by retroarch_ctl in ->, at line 6635 of RetroArch/retroarch.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that retroarch_ctl passes to ->, at line 6635 of RetroArch/retroarch.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	6826	6826
Object	->	->

Code Snippet	
File Name	RetroArch/retroarch.c
Method	bool retroarch_ctl(enum rarch_ctl_state state, void *data)

```
....
6826.                    sizeof(input_st->analog_requested));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=48
Status	New

The size of the buffer used by *rgui_init in ->, at line 6386 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *rgui_init passes to ->, at line 6386 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6521	6521
Object	->	->

Code Snippet
File Name RetroArch/rgui.c
Method static void *rgui_init(void **userdata, bool video_is_threaded)

```
....
6521.     memset(rgui->playlist_selection, 0, sizeof(rgui-
>playlist_selection));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=49
Status	New

The size of the buffer used by *rgui_init in menu_input_pointer_t, at line 6386 of RetroArch/rgui.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *rgui_init passes to menu_input_pointer_t, at line 6386 of RetroArch/rgui.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6529	6529
Object	menu_input_pointer_t	menu_input_pointer_t

Code Snippet
File Name RetroArch/rgui.c
Method static void *rgui_init(void **userdata, bool video_is_threaded)

```
....
6529.     memset(&rgui->pointer, 0, sizeof(menu_input_pointer_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=50
Status	New

The size of the buffer used by gl_glsl_destroy_resources in ->, at line 792 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_destroy_resources passes to ->, at line 792 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	817	817
Object	->	->

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_destroy_resources(glsl_shader_data_t *glsl)

```
....
817.     memset(glsl->prg, 0, sizeof(glsl->prg));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=51
Status	New

The size of the buffer used by gl_glsl_destroy_resources in ->, at line 792 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_destroy_resources passes to ->, at line 792 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	818	818
Object	->	->

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_destroy_resources(glsl_shader_data_t *glsl)

```
....
818.     memset(glsl->uniforms, 0, sizeof(glsl->uniforms));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=52
Status	New

The size of the buffer used by gl_glsl_destroy_resources in ->, at line 792 of RetroArch/shader_glsl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_glsl_destroy_resources passes to ->, at line 792 of RetroArch/shader_glsl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	835	835
Object	->	->

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_destroy_resources(glsl_shader_data_t *glsl)

```
....
835.     memset(&glsl->vbo, 0, sizeof(glsl->vbo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=53
Status	New

The size of the buffer used by ssl_parse_client_hello_v2 in ->, at line 838 of RetroArch/ssl_srv.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssl_parse_client_hello_v2 passes to ->, at line 838 of RetroArch/ssl_srv.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	980	980
Object	->	->

Code Snippet
File Name RetroArch/ssl_srv.c
Method static int ssl_parse_client_hello_v2(mbedtls_ssl_context *ssl)

```
....
980.              sizeof( ssl->session_negotiate->id ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=54
Status	New

The size of the buffer used by ssl_parse_client_hello in ->, at line 1103 of RetroArch/ssl_srv.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssl_parse_client_hello passes to ->, at line 1103 of RetroArch/ssl_srv.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	1437	1437
Object	->	->

Code Snippet
File Name RetroArch/ssl_srv.c
Method static int ssl_parse_client_hello(mbedtls_ssl_context *ssl)

```
....
1437.              sizeof( ssl->session_negotiate->id ) );
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=55
Status	New

The size of the buffer used by exynos_open in buf, at line 522 of RetroArch/exynos_gfx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that exynos_open passes to buf, at line 522 of RetroArch/exynos_gfx.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	563	563
Object	buf	buf

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_open(struct exynos_data *pdata)

```
....
563.     strncpy(pdata->drmname, buf, sizeof(buf));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=56
Status	New

The size of the buffer used by luaO_chunkid in l, at line 487 of RetroArch/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to l, at line 487 of RetroArch/lobject.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	491	491
Object	l	l

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
491.         memcpy(out, source + 1, l * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=57
Status	New

The size of the buffer used by luaO_chunkid in char, at line 487 of RetroArch/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 487 of RetroArch/lobject.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	491	491
Object	char	char

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
491.        memcpy(out, source + 1, l * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=58
Status	New

The size of the buffer used by luaO_chunkid in l, at line 487 of RetroArch/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to l, at line 487 of RetroArch/lobject.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	499	499
Object	l	l

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
499.        memcpy(out, source + 1, l * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=59
Status	New

The size of the buffer used by luaO_chunkid in char, at line 487 of RetroArch/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 487 of RetroArch/lobject.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	499	499
Object	char	char

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
499.        memcpy(out, source + 1, l * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=60
Status	New

The size of the buffer used by luaO_chunkid in bufflen, at line 487 of RetroArch/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to bufflen, at line 487 of RetroArch/lobject.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	503	503
Object	bufflen	bufflen

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
503.        memcpy(out, source + 1 + l - bufflen, bufflen *
sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=61
Status	New

The size of the buffer used by luaO_chunkid in char, at line 487 of RetroArch/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 487 of RetroArch/lobject.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	503	503
Object	char	char

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
503.        memcpy(out, source + 1 + l - bufflen, bufflen *
sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=62
Status	New

The size of the buffer used by luaO_chunkid in char, at line 487 of RetroArch/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 487 of RetroArch/lobject.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	519	519
Object	char	char

Code Snippet
File Name RetroArch/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t bufflen) {

```
....
519.      memcpy(out, POS, (LL(POS) + 1) * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=63
Status	New

The size of the buffer used by str_rep in l, at line 122 of RetroArch/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to l, at line 122 of RetroArch/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	135	135
Object	l	l

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
135.        memcpy(p, s, l * sizeof(char)); p += l;
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=64
Status	New

The size of the buffer used by str_rep in char, at line 122 of RetroArch/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to char, at line 122 of RetroArch/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	135	135
Object	char	char

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
135.        memcpy(p, s, l * sizeof(char)); p += l;
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=65
Status	New

The size of the buffer used by str_rep in lsep, at line 122 of RetroArch/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to lsep, at line 122 of RetroArch/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	137	137
Object	lsep	lsep

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
137.          memcpy(p, sep, lsep * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=66
Status	New

The size of the buffer used by str_rep in char, at line 122 of RetroArch/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to char, at line 122 of RetroArch/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	137	137
Object	char	char

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
137.          memcpy(p, sep, lsep * sizeof(char));
```

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=1010010&projectid=10011&pathid=1201
Status	New

The variable declared in save_ptr at RetroArch/config_file.c in line 652 is not initialized when it is used by line at RetroArch/config_file.c in line 652.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	658	667

Object	save_ptr	line

Code Snippet
File Name RetroArch/config_file.c
Method static int config_file_from_string_internal(

```
....
658.     char *save_ptr                  = NULL;
....
667.     line = strtok_r(lines, "\n", &save_ptr);
```

Use of Zero Initialized Pointer\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1202
Status New

The variable declared in entries_map at RetroArch/config_file.c in line 924 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	930	743
Object	entries_map	inc_tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
930.     conf->entries_map              = NULL;
```

File Name RetroArch/config_file.c
Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1203
Status New

The variable declared in path at RetroArch/config_file.c in line 924 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	929	743
Object	path	inc_tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
929.     conf->path                      = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1204
Status New

The variable declared in last at RetroArch/config_file.c in line 924 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	933	743
Object	last	inc_tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
933.     conf->last                      = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1205
Status New

The variable declared in references at RetroArch/config_file.c in line 924 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	934	743
Object	references	inc_tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
934.     conf->references                = NULL;
```

File Name RetroArch/config_file.c
Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1206
Status New

The variable declared in tail at RetroArch/config_file.c in line 924 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c

Line	932	743
Object	tail	inc_tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
932.     conf->tail                     = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1207
Status	New

The variable declared in entries at RetroArch/config_file.c in line 924 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	931	743
Object	entries	inc_tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
931.     conf->entries                  = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1208
Status	New

The variable declared in includes at RetroArch/config_file.c in line 924 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	935	743
Object	includes	inc_tmp

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
935.     conf->includes                  = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1209
Status	New

The variable declared in next at RetroArch/config_file.c in line 382 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	391	743
Object	next	inc_tmp

Code Snippet

File Name RetroArch/config_file.c

Method static void config_file_add_sub_conf(config_file_t *conf, char *path,

```
....
391.        node->next        = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1210
Status	New

The variable declared in conf at RetroArch/config_file.c in line 838 is not initialized when it is used by inc_tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	846	743
Object	conf	inc_tmp

Code Snippet

File Name RetroArch/config_file.c

Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
846.           config_file_t *conf           = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
743.     inc_tmp = (struct config_include_list*)conf->includes;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1211
Status	New

The variable declared in includes at RetroArch/config_file.c in line 924 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	935	724
Object	includes	tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
935.     conf->includes                  = NULL;
```

File Name RetroArch/config_file.c
Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1212
Status New

The variable declared in tail at RetroArch/config_file.c in line 924 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	932	724
Object	tail	tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
932.     conf->tail                      = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1213
Status	New

The variable declared in references at RetroArch/config_file.c in line 924 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	934	724
Object	references	tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
934.     conf->references                = NULL;
```

File Name RetroArch/config_file.c
Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1214
Status	New

The variable declared in path at RetroArch/config_file.c in line 924 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c

Line	929	724
Object	path	tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
929.     conf->path                      = NULL;
```

File Name RetroArch/config_file.c
Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1215
Status	New

The variable declared in entries_map at RetroArch/config_file.c in line 924 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	930	724
Object	entries_map	tmp

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
930.     conf->entries_map               = NULL;
```

File Name RetroArch/config_file.c
Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1216
Status	New

The variable declared in entries at RetroArch/config_file.c in line 924 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	931	724
Object	entries	tmp

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
931.     conf->entries                  = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1217
Status	New

The variable declared in last at RetroArch/config_file.c in line 924 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	933	724
Object	last	tmp

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
933.     conf->last                     = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1218
Status	New

The variable declared in next at RetroArch/config_file.c in line 382 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	391	724
Object	next	tmp

Code Snippet

File Name RetroArch/config_file.c

Method static void config_file_add_sub_conf(config_file_t *conf, char *path,

```
....
391.         node->next         = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1219
Status	New

The variable declared in conf at RetroArch/config_file.c in line 838 is not initialized when it is used by tmp at RetroArch/config_file.c in line 716.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	846	724
Object	conf	tmp

Code Snippet
File Name RetroArch/config_file.c
Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
846.           config_file_t *conf           = NULL;
```

File Name RetroArch/config_file.c

Method bool config_file_deinitialize(config_file_t *conf)

```
....
724.     tmp = conf->entries;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1220
Status	New

The variable declared in dst at RetroArch/exynos_gfx.c in line 436 is not initialized when it is used by dst at RetroArch/exynos_gfx.c in line 436.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	439	444
Object	dst	dst

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_g2d_init(struct exynos_data *pdata)

```
....
439.     struct g2d_image *dst = NULL;
....
444.     dst = calloc(1, sizeof(struct g2d_image));
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1221
Status	New

The variable declared in dst at RetroArch/exynos_gfx.c in line 436 is not initialized when it is used by src at RetroArch/exynos_gfx.c in line 436.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	439	480
Object	dst	src

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_g2d_init(struct exynos_data *pdata)

```
....
439.     struct g2d_image *dst = NULL;
....
480.         pdata->src[i]     = src;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1222
Status	New

The variable declared in dst at RetroArch/exynos_gfx.c in line 436 is not initialized when it is used by src at RetroArch/exynos_gfx.c in line 436.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	439	487
Object	dst	src

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_g2d_init(struct exynos_data *pdata)

```
....
439.     struct g2d_image *dst = NULL;
....
487.             free(pdata->src[i]);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1223
Status	New

The variable declared in page at RetroArch/exynos_gfx.c in line 820 is not initialized when it is used by page at RetroArch/exynos_gfx.c in line 1278.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	822	1308
Object	page	page

Code Snippet

File Name RetroArch/exynos_gfx.c

Method static struct exynos_page *exynos_free_page(struct exynos_data *pdata)

```
....
822.     struct exynos_page *page = NULL;
```

File Name RetroArch/exynos_gfx.c

Method static bool exynos_frame(void *data, const void *frame, unsigned width,

```
....
1308.        page = exynos_free_page(vid->data);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1224
Status	New

The variable declared in page at RetroArch/exynos_gfx.c in line 820 is not initialized when it is used by page at RetroArch/exynos_gfx.c in line 820.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	822	836
Object	page	page

Code Snippet

File Name RetroArch/exynos_gfx.c

Method static struct exynos_page *exynos_free_page(struct exynos_data *pdata)

```
....
822.     struct exynos_page *page = NULL;
....
836.     if (page->clear)
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1225
Status	New

The variable declared in page at RetroArch/exynos_gfx.c in line 820 is not initialized when it is used by page at RetroArch/exynos_gfx.c in line 820.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	822	834
Object	page	page

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static struct exynos_page *exynos_free_page(struct exynos_data *pdata)

```
....
822.     struct exynos_page *page = NULL;
....
834.     dst->bo[0] = page->bo->handle;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1226
Status	New

The variable declared in coreopts at RetroArch/menu_cbs_get_value.c in line 1612 is not initialized when it is used by desc at RetroArch/menu_cbs_get_value.c in line 1612.

	Source	Destination
File	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	1631	1634
Object	coreopts	desc

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_core_options(

```
....
1631.        core_option_manager_t *coreopts = NULL;
....
1634.           desc = core_option_manager_get_category_desc(
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1227
Status	New

The variable declared in input at RetroArch/midi_driver.c in line 249 is not initialized when it is used by input at RetroArch/midi_driver.c in line 249.

	Source	Destination
File	RetroArch/midi_driver.c	RetroArch/midi_driver.c
Line	266	315
Object	input	input

Code Snippet
File Name RetroArch/midi_driver.c
Method bool midi_driver_init(void *data)

```
....
266.        char * input  = NULL;
....
315.              rarch_midi_drv_input_enabled  = (input  != NULL);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1228
Status	New

The variable declared in output at RetroArch/midi_driver.c in line 249 is not initialized when it is used by output at RetroArch/midi_driver.c in line 249.

	Source	Destination
File	RetroArch/midi_driver.c	RetroArch/midi_driver.c
Line	267	316
Object	output	output

Code Snippet
File Name RetroArch/midi_driver.c
Method bool midi_driver_init(void *data)

```
....
267.        char * output = NULL;
....
316.              rarch_midi_drv_output_enabled = (output != NULL);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1229
Status	New

The variable declared in addr at RetroArch/net_http.c in line 426 is not initialized when it is used by state at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	428	850
Object	addr	state

Code Snippet

File Name RetroArch/net_http.c

Method static int net_http_new_socket(struct http_connection_t *conn)

```
....
428.     struct addrinfo *addr = NULL, *next_addr = NULL;
```

File Name RetroArch/net_http.c

Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
850.     state->sock_state = conn->sock_state;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1230
Status	New

The variable declared in core_info at RetroArch/retroarch.c in line 5322 is not initialized when it is used by core_info at RetroArch/retroarch.c in line 5322.

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c

Line	5327	5435
Object	core_info	core_info

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_parse_input_libretro_path(const char *path)

```
....
5327.     core_info_t *core_info = NULL;
....
5435.        core_path         = core_info->path;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1231
Status	New

The variable declared in line_metrics at RetroArch/switch_nx_gfx.c in line 248 is not initialized when it is used by line_metrics at RetroArch/switch_nx_gfx.c in line 248.

	Source	Destination
File	RetroArch/switch_nx_gfx.c	RetroArch/switch_nx_gfx.c
Line	255	258
Object	line_metrics	line_metrics

Code Snippet
File Name RetroArch/switch_nx_gfx.c
Method static void switch_font_render_message(

```
....
255.     struct font_line_metrics *line_metrics = NULL;
....
258.     line_height = scale / line_metrics->height;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1232
Status	New

The variable declared in entries_map at RetroArch/config_file.c in line 924 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination

File	RetroArch/config_file.c	RetroArch/config_file.c
Line	930	348
Object	entries_map	entries_map

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
930.     conf->entries_map               = NULL;
```

File Name RetroArch/config_file.c

Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1233
Status	New

The variable declared in includes at RetroArch/config_file.c in line 924 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	935	348
Object	includes	entries_map

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
935.     conf->includes                  = NULL;
```

File Name RetroArch/config_file.c

Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1234
Status	New

The variable declared in references at RetroArch/config_file.c in line 924 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	934	348
Object	references	entries_map

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
934.     conf->references                = NULL;
```

File Name RetroArch/config_file.c

Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1235
Status	New

The variable declared in last at RetroArch/config_file.c in line 924 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	933	348
Object	last	entries_map

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
933.     conf->last                     = NULL;
```

File Name RetroArch/config_file.c

Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1236
Status	New

The variable declared in tail at RetroArch/config_file.c in line 924 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	932	348
Object	tail	entries_map

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
932.     conf->tail                     = NULL;
```

File Name RetroArch/config_file.c

Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1237
Status	New

The variable declared in entries at RetroArch/config_file.c in line 924 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	931	348
Object	entries	entries_map

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
931.     conf->entries                  = NULL;
```

File Name RetroArch/config_file.c
Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1238
Status New

The variable declared in path at RetroArch/config_file.c in line 924 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	929	348
Object	path	entries_map

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
929.     conf->path                     = NULL;
```

File Name RetroArch/config_file.c

Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1239
Status	New

The variable declared in next at RetroArch/config_file.c in line 382 is not initialized when it is used by entries_map at RetroArch/config_file.c in line 268.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	391	348
Object	next	entries_map

Code Snippet
File Name RetroArch/config_file.c
Method static void config_file_add_sub_conf(config_file_t *conf, char *path,

```
....
391.        node->next        = NULL;
```

File Name RetroArch/config_file.c

Method static void config_file_add_child_list(config_file_t *parent,

```
....
348.        parent->entries_map = child->entries_map;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1240
Status	New

The variable declared in next at RetroArch/config_file.c in line 382 is not initialized when it is used by next at RetroArch/config_file.c in line 382.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c

Line	391	400
Object	next	next

Code Snippet
File Name RetroArch/config_file.c
Method static void config_file_add_sub_conf(config_file_t *conf, char *path,

```
....
391.         node->next         = NULL;
....
400.            head->next      = node;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1241
Status	New

The variable declared in entries at RetroArch/config_file.c in line 782 is not initialized when it is used by entries at RetroArch/config_file.c in line 782.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	809	808
Object	entries	entries

Code Snippet
File Name RetroArch/config_file.c
Method bool config_append_file(config_file_t *conf, const char *path)

```
....
809.         new_conf->entries     = NULL;
....
808.         conf->entries         = new_conf->entries; /* Pilfer. */
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1242
Status	New

The variable declared in last at RetroArch/config_file.c in line 924 is not initialized when it is used by conf at RetroArch/config_file.c in line 838.

	Source	Destination

File	RetroArch/config_file.c	RetroArch/config_file.c
Line	933	851
Object	last	conf

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
933.     conf->last                     = NULL;
```

File Name RetroArch/config_file.c
Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
851.              conf = config_file_new_from_string((char*)ret_buf,
path);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1243
Status	New

The variable declared in references at RetroArch/config_file.c in line 924 is not initialized when it is used by conf at RetroArch/config_file.c in line 838.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	934	851
Object	references	conf

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
934.     conf->references               = NULL;
```

File Name RetroArch/config_file.c
Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
851.              conf = config_file_new_from_string((char*)ret_buf,
path);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1244
Status	New

The variable declared in tail at RetroArch/config_file.c in line 924 is not initialized when it is used by conf at RetroArch/config_file.c in line 838.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	932	851
Object	tail	conf

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
932.     conf->tail                      = NULL;
```

File Name RetroArch/config_file.c

Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
851.              conf = config_file_new_from_string((char*)ret_buf,
path);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1245
Status	New

The variable declared in entries at RetroArch/config_file.c in line 924 is not initialized when it is used by conf at RetroArch/config_file.c in line 838.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c

Line	931	851
Object	entries	conf

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
931.     conf->entries                  = NULL;
```

File Name RetroArch/config_file.c

Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
851.             conf = config_file_new_from_string((char*)ret_buf,
path);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1246
Status	New

The variable declared in entries_map at RetroArch/config_file.c in line 924 is not initialized when it is used by conf at RetroArch/config_file.c in line 838.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	930	851
Object	entries_map	conf

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_initialize(struct config_file *conf)

```
....
930.     conf->entries_map              = NULL;
```

File Name RetroArch/config_file.c

Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
851.             conf = config_file_new_from_string((char*)ret_buf,
path);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1247
Status	New

The variable declared in includes at RetroArch/config_file.c in line 924 is not initialized when it is used by conf at RetroArch/config_file.c in line 838.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	935	851
Object	includes	conf

Code Snippet

File Name RetroArch/config_file.c

Method void config_file_initialize(struct config_file *conf)

```
....
935.     conf->includes                  = NULL;
```

File Name RetroArch/config_file.c

Method config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
851.              conf = config_file_new_from_string((char*)ret_buf,
path);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1248
Status	New

The variable declared in path at RetroArch/config_file.c in line 924 is not initialized when it is used by conf at RetroArch/config_file.c in line 838.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	929	851
Object	path	conf

Code Snippet

File Name	RetroArch/config_file.c
Method	void config_file_initialize(struct config_file *conf)

```
....
929.      conf->path                      = NULL;
```

File Name	RetroArch/config_file.c
Method	config_file_t *config_file_new_from_path_to_string(const char *path)

```
....
851.               conf = config_file_new_from_string((char*)ret_buf,
path);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1249
Status	New

The variable declared in next at RetroArch/config_file.c in line 1234 is not initialized when it is used by entries at RetroArch/config_file.c in line 1234.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1284	1290
Object	next	entries

Code Snippet

File Name	RetroArch/config_file.c
Method	void config_set_string(config_file_t *conf, const char *key, const char *val)

```
....
1284.      entry->next      = NULL;
....
1290.         conf->entries = entry;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1250
Status	New

The variable declared in Pointer at RetroArch/drm_gfx.c in line 193 is not initialized when it is used by surface at RetroArch/drm_gfx.c in line 215.

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	205	226
Object	Pointer	surface

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_surface_free(void *data, struct drm_surface **sp)

```
....
205.     *sp = NULL;
```

File Name RetroArch/drm_gfx.c
Method static void drm_surface_setup(void *data, int src_width, int src_height,

```
....
226.     surface = *sp;
```

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=1010010&projectid=10011&pathid=920
Status New

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	8607	8607
Object	arraySizes	arraySizes

Code Snippet
File Name RetroArch/Initialize.cpp
Method void TBuiltIns::identifyBuiltIns(int version, EProfile profile, const SpvVersion& spvVersion, EShLanguage language, TSymbolTable& symbolTable, const TBuiltInResource &resources)

```
....
8607.              TArraySizes* arraySizes = new TArraySizes;
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=921
Status	New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	641	641
Object	value	value

Code Snippet
File Name RetroArch/config_file.c
Method static bool config_file_parse_line(config_file_t *conf,

```
....
641.     if (!(list->value    = config_file_extract_value(line)))
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=922
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7286	7286
Object	xmb_path_dynamic_wallpaper	xmb_path_dynamic_wallpaper

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_context_reset_background(xmb_handle_t *xmb, const char *iconpath)

```
....
7286.         strlcpy(path, xmb_path_dynamic_wallpaper(xmb),
sizeof(path));
```

Memory Leak\Path 4:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=923
Status	New

	Source	Destination
File	RetroArch/bitmapfont.c	RetroArch/bitmapfont.c
Line	177	177
Object	handle	handle

Code Snippet
File Name RetroArch/bitmapfont.c
Method static void *font_renderer_bmp_init(const char *font_path, float font_size)

```
....
177.     bm_renderer_t *handle = (bm_renderer_t*)calloc(1,
sizeof(*handle));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=924
Status	New

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	847	847
Object	frame_output	frame_output

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_set_texture_frame(void *data, const void *frame, bool rgb32,

```
....
847.     char *frame_output = (char *) malloc (dst_pitch * height);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=925
Status	New

	Source	Destination

File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	1058	1058
Object	state	state

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static STATE_T *read_state(const char *dir)

```
....
1058.       STATE_T *state = malloc(sizeof(STATE_T));
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=926
Status New

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	494	494
Object	model	model

Code Snippet
File Name RetroArch/models.c
Method MODEL_T cube_wavefront(void)

```
....
494.      WAVEFRONT_MODEL_T *model = malloc(sizeof *model);
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=927
Status New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	637	637
Object	urlcopy	urlcopy

Code Snippet
File Name RetroArch/net_http.c
Method bool net_http_connection_done(struct http_connection_t *conn)

```
....
637.            char* urlcopy       = (char*)malloc(domain_len +
location_len + 2);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=928
Status	New

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	1060	1060
Object	newhost	newhost

Code Snippet
File Name RetroArch/rc_api_common.c
Method static void rc_api_update_host(char** host, const char* hostname) {

```
....
1060.           char* newhost = (char*)malloc(hostname_len + 7 + 1);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=929
Status	New

	Source	Destination
File	RetroArch/switch_nx_gfx.c	RetroArch/switch_nx_gfx.c
Line	492	492
Object	sw	sw

Code Snippet
File Name RetroArch/switch_nx_gfx.c
Method static void *switch_init(const video_info_t *video,

```
....
492.       switch_video_t *sw = (switch_video_t *)calloc(1, sizeof(*sw));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=930
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	625	625
Object	new_node	new_node

Code Snippet
File Name RetroArch/xmb.c
Method static xmb_node_t *xmb_copy_node(const xmb_node_t *old_node)

```
....
625.     xmb_node_t *new_node = (xmb_node_t*)malloc(sizeof(*new_node));
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=931
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7553	7553
Object	data	data

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_list_deep_copy(const file_list_t *src, file_list_t *dst,

```
....
7553.           void *data = malloc(sizeof(menu_file_list_cbs_t));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=932
Status	New

	Source	Destination
File	RetroArch/bitmapfont.c	RetroArch/bitmapfont.c

Line	58	58
Object	font	font

Code Snippet
File Name RetroArch/bitmapfont.c
Method bitmapfont_lut_t *bitmapfont_get_lut(void)

```
....
58.     font = (bitmapfont_lut_t*)calloc(1, sizeof(bitmapfont_lut_t));
```

Memory Leak\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=933
Status New

	Source	Destination
File	RetroArch/bitmapfont.c	RetroArch/bitmapfont.c
Line	68	68
Object	lut	lut

Code Snippet
File Name RetroArch/bitmapfont.c
Method bitmapfont_lut_t *bitmapfont_get_lut(void)

```
....
68.     font->lut = (bool**)calloc(1, BMP_ATLAS_SIZE * sizeof(bool*));
```

Memory Leak\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=934
Status New

	Source	Destination
File	RetroArch/bitmapfont.c	RetroArch/bitmapfont.c
Line	190	190
Object	buffer	buffer

Code Snippet
File Name RetroArch/bitmapfont.c
Method static void *font_renderer_bmp_init(const char *font_path, float font_size)

```
....
190.     handle->atlas.buffer = (uint8_t*)calloc(handle->atlas.width *
handle->atlas.height, 1);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=935
Status	New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	662	662
Object	path	path

Code Snippet
File Name RetroArch/config_file.c
Method static int config_file_from_string_internal(

```
....
662.         conf->path                    = strdup(path);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=936
Status	New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1269	1269
Object	value	value

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_string(config_file_t *conf, const char *key, const char *val)

```
....
1269.            entry->value    = strdup(val);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=937
Status	New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1278	1278
Object	entry	entry

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_string(config_file_t *conf, const char *key, const char *val)

```
....
1278.     if (!(entry = (struct
config_entry_list*)malloc(sizeof(*entry))))
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=938
Status	New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1282	1282
Object	key	key

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_string(config_file_t *conf, const char *key, const char *val)

```
....
1282.     entry->key       = strdup(key);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=939
Status	New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c

Line	1283	1283
Object	value	value

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_string(config_file_t *conf, const char *key, const char *val)

```
....
1283.     entry->value     = strdup(val);
```

Memory Leak\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=940
Status New

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	245	245
Object	pages	pages

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_surface_setup(void *data, int src_width, int src_height,

```
....
245.     surface->pages = (struct drm_page*)
```

Memory Leak\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=941
Status New

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	786	786
Object	dh	dh

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int dtoverlay_list_all(STATE_T *state)

```
....
786.      dh = opendir(overlay_src_dir);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=942
Status	New

	Source	Destination
File	RetroArch/flv_reader.c	RetroArch/flv_reader.c
Line	1023	1023
Object	module	module

Code Snippet
File Name RetroArch/flv_reader.c
Method VC_CONTAINER_STATUS_T flv_reader_open(VC_CONTAINER_T *p_ctx)

```
....
1023.     module = malloc(sizeof(*module));
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=943
Status	New

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	368	368
Object	model	model

Code Snippet
File Name RetroArch/models.c
Method MODEL_T load_wavefront(const char *modelname, const char *texturename)

```
....
368.     model = malloc(sizeof *model);
```

Memory Leak\Path 25:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=944
Status	New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	531	531
Object	methodcopy	methodcopy

Code Snippet
File Name RetroArch/net_http.c
Method struct http_connection_t *net_http_connection_new(const char *url,

```
....
531.        conn->methodcopy     = strdup(method);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=945
Status	New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	534	534
Object	postdatacopy	postdatacopy

Code Snippet
File Name RetroArch/net_http.c
Method struct http_connection_t *net_http_connection_new(const char *url,

```
....
534.        conn->postdatacopy   = strdup(data);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=946
Status	New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	536	536

Object	urlcopy	urlcopy

Code Snippet
File Name RetroArch/net_http.c
Method struct http_connection_t *net_http_connection_new(const char *url,

```
....
536.     if (!(conn->urlcopy = strdup(url)))
```

Memory Leak\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=947
Status New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	695	695
Object	useragentcopy	useragentcopy

Code Snippet
File Name RetroArch/net_http.c
Method void net_http_connection_set_user_agent(

```
....
695.     conn->useragentcopy = user_agent ? strdup(user_agent) : NULL;
```

Memory Leak\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=948
Status New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	704	704
Object	headerscopy	headerscopy

Code Snippet
File Name RetroArch/net_http.c
Method void net_http_connection_set_headers(

```
....
704.     conn->headerscopy = headers ? strdup(headers) : NULL;
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=949
Status	New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	860	860
Object	data	data

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
860.     if (!(state->data = (char*)malloc(state->buflen)))
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=950
Status	New

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	800	800
Object	next	next

Code Snippet
File Name RetroArch/rc_api_common.c
Method char* rc_buf_reserve(rc_api_buffer_t* buffer, size_t amount) {

```
....
800.         chunk->next = (rc_api_buffer_chunk_t*)malloc(alloc_size);
```

Memory Leak\Path 32:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=951
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5952	5952
Object	connect_host	connect_host

Code Snippet
File Name RetroArch/retroarch.c
Method static bool retroarch_parse_input_and_config(

```
....
5952.                  p_rarch->connect_host = strdup(optarg);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=952
Status	New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6287	6287
Object	data	data

Code Snippet
File Name RetroArch/rgui.c
Method static bool rgui_set_aspect_ratio(

```
....
6287.      rgui->frame_buf.data = (uint16_t*)calloc(
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=953
Status	New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6312	6312

Object	data	data

Code Snippet
File Name RetroArch/rgui.c
Method static bool rgui_set_aspect_ratio(

```
....
6312.     rgui->background_buf.data      = (uint16_t*)calloc(
```

Memory Leak\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=954
Status New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6321	6321
Object	data	data

Code Snippet
File Name RetroArch/rgui.c
Method static bool rgui_set_aspect_ratio(

```
....
6321.     rgui->fs_thumbnail.data        = (uint16_t*)calloc(
```

Memory Leak\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=955
Status New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6336	6336
Object	data	data

Code Snippet
File Name RetroArch/rgui.c
Method static bool rgui_set_aspect_ratio(

```
....
6336.     rgui->mini_thumbnail.data            = (uint16_t*)calloc(
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=956
Status	New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6344	6344
Object	data	data

Code Snippet
File Name RetroArch/rgui.c
Method static bool rgui_set_aspect_ratio(

```
....
6344.     rgui->mini_left_thumbnail.data       = (uint16_t*)calloc(
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=957
Status	New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6408	6408
Object	rgui	rgui

Code Snippet
File Name RetroArch/rgui.c
Method static void *rgui_init(void **userdata, bool video_is_threaded)

```
....
6408.     if (!(rgui = (rgui_t*)calloc(1, sizeof(rgui_t))))
```

Memory Leak\Path 39:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=958
Status	New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	6661	6661
Object	data	data

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_set_texture(void *data)

```
....
6661.              if (!(upscale_buf->data = (uint16_t*)
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=959
Status	New

	Source	Destination
File	RetroArch/rtp_mpeg4.c	RetroArch/rtp_mpeg4.c
Line	745	745
Object	extra	extra

Code Snippet
File Name RetroArch/rtp_mpeg4.c
Method VC_CONTAINER_STATUS_T mp4_parameter_handler(VC_CONTAINER_T *p_ctx,

```
....
745.     extra = (MP4_PAYLOAD_T *)malloc(sizeof(MP4_PAYLOAD_T));
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=960
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	565	565

Object	fragment	fragment

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_load_source_path(struct video_shader_pass *pass,

```
....
565.     pass->source.string.fragment = strdup(pass-
>source.string.vertex);
```

Memory Leak\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=961
Status New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1019	1019
Object	shader	shader

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void *gl_glsl_init(void *data, const char *path)

```
....
1019.     glsl->shader = (struct video_shader*)calloc(1, sizeof(*glsl-
>shader));
```

Memory Leak\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=962
Status New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1063	1063
Object	vertex	vertex

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void *gl_glsl_init(void *data, const char *path)

```
....
1063.           glsl->shader->pass[0].source.string.vertex   =
strdup(stock_vertex_modern);
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=963
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1064	1064
Object	fragment	fragment

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void *gl_glsl_init(void *data, const char *path)

```
....
1064.           glsl->shader->pass[0].source.string.fragment =
strdup(stock_fragment_modern);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=964
Status	New

	Source	Destination
File	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	57	57
Object	cli_id	cli_id

Code Snippet
File Name RetroArch/ssl_srv.c
Method int mbedtls_ssl_set_client_transport_id(mbedtls_ssl_context *ssl,

```
....
57.      if( ( ssl->cli_id = (unsigned char*)calloc( 1, ilen ) ) == NULL
)
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=965
Status	New

	Source	Destination
File	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	261	261
Object	curves	curves

Code Snippet
File Name RetroArch/ssl_srv.c
Method static int ssl_parse_supported_elliptic_curves(mbedtls_ssl_context *ssl,

```
....
261.      if( ( curves = (const mbedtls_ecp_curve_info**)
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=966
Status	New

	Source	Destination
File	RetroArch/switch_nx_gfx.c	RetroArch/switch_nx_gfx.c
Line	872	872
Object	pixels	pixels

Code Snippet
File Name RetroArch/switch_nx_gfx.c
Method static void switch_set_texture_frame(

```
....
872.              sw->menu_texture.pixels = malloc(sz);
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=967
Status	New

	Source	Destination

File	RetroArch/wav_reader.c	RetroArch/wav_reader.c
Line	257	257
Object	module	module

Code Snippet
File Name RetroArch/wav_reader.c
Method VC_CONTAINER_STATUS_T wav_reader_open(VC_CONTAINER_T *p_ctx)

```
....
257.     module = malloc(sizeof(*module));
```

Memory Leak\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=968
Status New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	631	631
Object	fullpath	fullpath

Code Snippet
File Name RetroArch/xmb.c
Method static xmb_node_t *xmb_copy_node(const xmb_node_t *old_node)

```
....
631.     new_node->fullpath     = old_node->fullpath ? strdup(old_node->fullpath) : NULL;
```

Memory Leak\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=969
Status New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	632	632
Object	console_name	console_name

Code Snippet
File Name RetroArch/xmb.c

Method	static xmb_node_t *xmb_copy_node(const xmb_node_t *old_node)

```
....
632.     new_node->console_name = old_node->console_name ?
strdup(old_node->console_name) : NULL;
```

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=1010010&projectid=10011&pathid=1284
Status	New

The size of the buffer used by SB_set_length in len, at line 171 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	651	175
Object	fgetc	len

Code Snippet

File Name	RetroArch/test_x509.c
Method	conf_next_low(void)

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

File Name	RetroArch/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=1010010&projectid=100

	11&pathid=1285
Status	New

The size of the buffer used by SB_set_length in len, at line 171 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	657	175
Object	fgetc	len

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=1286
Status	New

The size of the buffer used by SB_set_length in BinaryExpr, at line 171 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	651	175
Object	fgetc	BinaryExpr

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=1287
Status	New

The size of the buffer used by SB_set_length in BinaryExpr, at line 171 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	657	175
Object	fgetc	BinaryExpr

Code Snippet

File Name RetroArch/test_x509.c

Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=1288
Status	New

The size of the buffer used by SB_set_length in ptr, at line 171 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	651	175
Object	fgetc	ptr

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=1289
Status	New

The size of the buffer used by SB_set_length in ptr, at line 171 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	657	175
Object	fgetc	ptr

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=1290
Status	New

The size of the buffer used by SB_expand in ptr, at line 106 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	651	119
Object	fgetc	ptr

Code Snippet

File Name RetroArch/test_x509.c

Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=1291
Status	New

The size of the buffer used by SB_expand in ptr, at line 106 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	657	119

Object	fgetc	ptr

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=1292
Status	New

The size of the buffer used by overlay_applied in status, at line 1022 of RetroArch/dtoverlay_main.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that overlay_applied passes to status, at line 1022 of RetroArch/dtoverlay_main.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	1030	1035
Object	status	status

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int overlay_applied(const char *overlay_dir)

```
....
1030.       bytes = fread(status, 1, sizeof(status), fp);
....
1035.       (memcmp(status, "applied", sizeof(status)) == 0);
```

Stored Buffer Overflow boundcpy\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1293
Status	New

The size of the buffer used by overlay_applied in sizeof, at line 1022 of RetroArch/dtoverlay_main.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that overlay_applied passes to status, at line 1022 of RetroArch/dtoverlay_main.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	1030	1035
Object	status	sizeof

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int overlay_applied(const char *overlay_dir)

```
....
1030.       bytes = fread(status, 1, sizeof(status), fp);
....
1035.       (memcmp(status, "applied", sizeof(status)) == 0);
```

Stored Buffer Overflow boundcpy\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1294
Status New

The size of the buffer used by HomebrewCopyMemory in bytes, at line 111 of RetroArch/hbl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that HBL_loadToMemory passes to BinaryExpr, at line 243 of RetroArch/hbl.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c
Line	276	144
Object	BinaryExpr	bytes

Code Snippet
File Name RetroArch/hbl.c
Method int HBL_loadToMemory(const char *filepath, u32 args_size)

```
....
276.        ret = fread(buffer + bytesRead, 1, blockSize, fp);
```

File Name RetroArch/hbl.c
Method static int HomebrewCopyMemory(u8 *address, u32 bytes, u32 args_size)

```
....
144.        memcpy((void *)ELF_DATA_ADDR, address, bytes);
```

Stored Buffer Overflow boundcpy\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1295
Status	New

The size of the buffer used by load_wavefront_obj in valid, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	316
Object	line	valid

Code Snippet

File Name RetroArch/models.c

Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
316.        memmove(line, end, valid - i);
```

Stored Buffer Overflow boundcpy\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1296
Status	New

The size of the buffer used by load_wavefront_obj in valid, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	316
Object	BinaryExpr	valid

Code Snippet

File Name RetroArch/models.c

Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
316.        memmove(line, end, valid - i);
```

Stored Buffer Overflow boundcpy\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1297
Status	New

The size of the buffer used by load_wavefront_obj in BinaryExpr, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	316
Object	line	BinaryExpr

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
316.        memmove(line, end, valid - i);
```

Stored Buffer Overflow boundcpy\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1298
Status	New

The size of the buffer used by load_wavefront_obj in BinaryExpr, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	316
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
316.        memmove(line, end, valid - i);
```

Stored Buffer Overflow boundcpy\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1299
Status	New

The size of the buffer used by load_wavefront_obj in i, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	316
Object	line	i

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
316.        memmove(line, end, valid - i);
```

Stored Buffer Overflow boundcpy\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1300
Status	New

The size of the buffer used by load_wavefront_obj in i, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	316

Object	BinaryExpr	i

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
316.        memmove(line, end, valid - i);
```

Stored Buffer Overflow boundcpy\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1301
Status	New

The size of the buffer used by load_wavefront_obj in numt, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	335
Object	line	numt

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1302
Status	New

The size of the buffer used by load_wavefront_obj in numt, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination

File	RetroArch/models.c	RetroArch/models.c
Line	318	335
Object	BinaryExpr	numt

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1303
Status	New

The size of the buffer used by load_wavefront_obj in BinaryExpr, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	335
Object	line	BinaryExpr

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1304
Status	New

The size of the buffer used by load_wavefront_obj in BinaryExpr, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	335
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1305
Status New

The size of the buffer used by load_wavefront_obj in Pointer, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	336
Object	line	Pointer

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1306
Status	New

The size of the buffer used by load_wavefront_obj in Pointer, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	336
Object	BinaryExpr	Pointer

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.         valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1307
Status	New

The size of the buffer used by load_wavefront_obj in qn, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	336
Object	line	qn

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1308
Status	New

The size of the buffer used by load_wavefront_obj in qn, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	336
Object	BinaryExpr	qn

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.         valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1309
Status	New

The size of the buffer used by load_wavefront_obj in sizeof, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	336
Object	line	sizeof

Code Snippet	
File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1310
Status	New

The size of the buffer used by load_wavefront_obj in sizeof, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	336
Object	BinaryExpr	sizeof

Code Snippet	
File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.         valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1311
Status	New

The size of the buffer used by load_wavefront_obj in BinaryExpr, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination

File	RetroArch/models.c	RetroArch/models.c
Line	226	336
Object	line	BinaryExpr

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data + (3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1312
Status	New

The size of the buffer used by load_wavefront_obj in BinaryExpr, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	336
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.         valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data + (3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1313
Status	New

The size of the buffer used by load_wavefront_obj in numn, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	336
Object	line	numn

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1314
Status New

The size of the buffer used by load_wavefront_obj in numn, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	336
Object	BinaryExpr	numn

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.         valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
336.     memcpy((float *)m->data + m->numv + m->numt,(float *) m->data +
(3 + 2) * MAX_VERTICES, m->numn * sizeof *qn);
```

Stored Buffer Overflow boundcpy\Path 32:

Severity Medium
Result State To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1315
Status	New

The size of the buffer used by load_wavefront_obj in Pointer, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	335
Object	line	Pointer

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1316
Status	New

The size of the buffer used by load_wavefront_obj in Pointer, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	335
Object	BinaryExpr	Pointer

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1317
Status	New

The size of the buffer used by load_wavefront_obj in qt, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	335
Object	line	qt

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1318
Status	New

The size of the buffer used by load_wavefront_obj in qt, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	335
Object	BinaryExpr	qt

Code Snippet	
File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1319
Status	New

The size of the buffer used by load_wavefront_obj in sizeof, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to line, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	335
Object	line	sizeof

Code Snippet	
File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1320
Status	New

The size of the buffer used by load_wavefront_obj in sizeof, at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to BinaryExpr, at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c

Line	318	335
Object	BinaryExpr	sizeof

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.         valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
....
335.     memcpy((float *)m->data + m->numv, (float *)m->data + 3 *
MAX_VERTICES, m->numt * sizeof *qt);
```

Stored Buffer Overflow boundcpy\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1321
Status	New

The size of the buffer used by eqpkey in key, at line 1408 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	423	1429
Object	BinaryExpr	key

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

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

File Name RetroArch/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;
```

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=1010010&projectid=10011&pathid=472
Status	New

The function alloc_size in RetroArch/rc_api_common.c at line 786 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	800	800
Object	alloc_size	alloc_size

Code Snippet
File Name RetroArch/rc_api_common.c
Method char* rc_buf_reserve(rc_api_buffer_t* buffer, size_t amount) {

```
....
800.        chunk->next = (rc_api_buffer_chunk_t*)malloc(alloc_size);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=473
Status	New

The function elems in RetroArch/shader_glsl.c at line 1555 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	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1588	1588
Object	elems	elems

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_set_coords(void *shader_data,

```
....
1588.        buffer        = (GLfloat*)malloc(elems);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=474
Status	New

The function len in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	56	56
Object	len	len

Code Snippet
File Name RetroArch/test_x509.c
Method xmalloc(size_t len)

```
....
56.   buf = malloc(len);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=475
Status	New

The function len in RetroArch/cdrom.c at line 1025 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	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1081	1081
Object	len	len

Code Snippet
File Name RetroArch/cdrom.c
Method int cdrom_write_cue(libretro_vfs_implementation_file *stream, char **out_buf, size_t *out_len, char cdrom_drive, unsigned char *num_tracks, cdrom_toc_t *toc)

```
....
1081.      *out_buf = (char*)calloc(1, len);
```

Wrong Size t Allocation\Path 5:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=476
Status	New

The function ilen in RetroArch/ssl_srv.c at line 48 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	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	57	57
Object	ilen	ilen

Code Snippet
File Name RetroArch/ssl_srv.c
Method int mbedtls_ssl_set_client_transport_id(mbedtls_ssl_context *ssl,

```
....
57.      if( ( ssl->cli_id = (unsigned char*)calloc( 1, ilen ) ) == NULL
)
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=477
Status	New

The function our_size in RetroArch/ssl_srv.c at line 228 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	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	262	262
Object	our_size	our_size

Code Snippet
File Name RetroArch/ssl_srv.c
Method static int ssl_parse_supported_elliptic_curves(mbedtls_ssl_context *ssl,

```
....
262.              calloc( our_size, sizeof( *curves ) ) ) == NULL )
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=478

Status	New

The function n in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	83	83
Object	n	n

Code Snippet
File Name RetroArch/test_x509.c
Method xstrdup(const char *name)

```
....
83.    s = xmalloc(n);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=479
Status	New

The function nlen in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	118	118
Object	nlen	nlen

Code Snippet
File Name RetroArch/test_x509.c
Method SB_expand(string_builder *sb, size_t extra_len)

```
....
118.         nbuf = xmalloc(nlen);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=480
Status	New

The function blen in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	409	409
Object	blen	blen

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

```
....
409.        buf = xmalloc(blen);
```

Wrong Size t Allocation\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=481
Status New

The function blen in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	418	418
Object	blen	blen

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

```
....
418.                    buf2 = xmalloc(blen);
```

Wrong Size t Allocation\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=482
Status New

The function ptr in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	427	427
Object	ptr	ptr

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

```
....
427.                    buf3 = xmalloc(ptr);
```

Wrong Size t Allocation\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=483
Status New

The function ptr in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1022	1022
Object	ptr	ptr

Code Snippet
File Name RetroArch/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 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=484
Status New

The function len in RetroArch/net_http.c at line 717 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	RetroArch/net_http.c	RetroArch/net_http.c

Line	808	808
Object	len	len

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
808.        len_str = (char*)malloc(len + 1);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=485
Status	New

The function len in RetroArch/test_x509.c at line 1985 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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	2013	2013
Object	len	len

Code Snippet
File Name RetroArch/test_x509.c
Method main(int argc, const char *argv[])

```
....
2013.                        dn = xmalloc(len + 1);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=486
Status	New

The function n2 in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	272	272
Object	n2	n2

Code Snippet	
File Name	RetroArch/test_x509.c
Method	HT_expand(HT *ht)

```
....
272.        new_buckets = xmalloc(n2 * sizeof *new_buckets);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=487
Status	New

The function len in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	817	817
Object	len	len

Code Snippet	
File Name	RetroArch/test_x509.c
Method	parse_header_name(void)

```
....
817.        name = xmalloc(len + 1);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=488
Status	New

The function u in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	844	844
Object	u	u

Code Snippet	
File Name	RetroArch/test_x509.c

Method	parse_keyvalue(HT *d)

```
....
844.        name = xmalloc(u + 1);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=489
Status	New

The function all_chains_len in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1300	1300
Object	all_chains_len	all_chains_len

Code Snippet	
File Name	RetroArch/test_x509.c
Method	parse_object(char *objtype, HT *objdata, long linenum)

```
....
1300.                                   all_chains_len * sizeof
*all_chains);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=490
Status	New

The function nlen in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1306	1306
Object	nlen	nlen

Code Snippet	
File Name	RetroArch/test_x509.c
Method	parse_object(char *objtype, HT *objdata, long linenum)

```
....
1306.                          ntc = xmalloc(nlen * sizeof *ntc);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=491
Status	New

The function num_anchors in RetroArch/test_x509.c at line 1442 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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1476	1476
Object	num_anchors	num_anchors

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1476.       anchors = xmalloc(num_anchors * sizeof *anchors);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=492
Status	New

The function num_certs in RetroArch/test_x509.c at line 1442 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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1503	1503
Object	num_certs	num_certs

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1503.       certs = xmalloc(num_certs * sizeof *certs);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=493
Status	New

The function num_names in RetroArch/test_x509.c at line 1800 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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1829	1829
Object	num_names	num_names

Code Snippet
File Name RetroArch/test_x509.c
Method test_name_extraction(void)

```
....
1829.       names = xmalloc(num_names * sizeof *names);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=494
Status	New

The function domain_len in RetroArch/net_http.c at line 586 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	RetroArch/net_http.c	RetroArch/net_http.c
Line	637	637
Object	domain_len	domain_len

Code Snippet
File Name RetroArch/net_http.c
Method bool net_http_connection_done(struct http_connection_t *conn)

```
....
637.            char* urlcopy       = (char*)malloc(domain_len +
location_len + 2);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=495
Status	New

The function location_len in RetroArch/net_http.c at line 586 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	RetroArch/net_http.c	RetroArch/net_http.c
Line	637	637
Object	location_len	location_len

Code Snippet
File Name RetroArch/net_http.c
Method bool net_http_connection_done(struct http_connection_t *conn)

```
....
637.            char* urlcopy       = (char*)malloc(domain_len +
location_len + 2);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=496
Status	New

The function hostname_len in RetroArch/rc_api_common.c at line 1046 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	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	1060	1060
Object	hostname_len	hostname_len

Code Snippet
File Name RetroArch/rc_api_common.c
Method static void rc_api_update_host(char** host, const char* hostname) {

```
....
1060.          char* newhost = (char*)malloc(hostname_len + 7 + 1);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=497
Status	New

The function len in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	862	862
Object	len	len

Code Snippet
File Name RetroArch/test_x509.c
Method parse_keyvalue(HT *d)

```
....
862.        value = xmalloc(len - u + 1);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=498
Status	New

The function u in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	862	862
Object	u	u

Code Snippet
File Name RetroArch/test_x509.c
Method parse_keyvalue(HT *d)

```
....
862.        value = xmalloc(len - u + 1);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=499
Status	New

The function v in RetroArch/test_x509.c at line 1031 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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1057	1057
Object	v	v

Code Snippet
File Name RetroArch/test_x509.c
Method split_names(const char *value)

```
....
1057.                                   name = xmalloc(v - u + 1);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=500
Status	New

The function u in RetroArch/test_x509.c at line 1031 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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1057	1057
Object	u	u

Code Snippet
File Name RetroArch/test_x509.c
Method split_names(const char *value)

```
....
1057.                                   name = xmalloc(v - u + 1);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=501
Status	New

The function ptr in RetroArch/test_x509.c at line 1031 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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1067	1067
Object	ptr	ptr

Code Snippet
File Name RetroArch/test_x509.c
Method split_names(const char *value)

```
....
1067.                   names = xmalloc((ptr + 1) * sizeof *names);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=502
Status	New

The function linenum in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1254	1254
Object	linenum	linenum

Code Snippet
File Name RetroArch/test_x509.c
Method parse_object(char *objtype, HT *objdata, long linenum)

```
....
1254.                          get_value(objtype, objdata, linenum,
"eekey"));
```

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=1010010&projectid=10011&pathid=452
Status	New

Calling free() (line 218) on a variable that was not dynamically allocated (line 218) in file RetroArch/bitmapfont.c may result with a crash.

	Source	Destination
File	RetroArch/bitmapfont.c	RetroArch/bitmapfont.c
Line	224	224
Object	handle	handle

Code Snippet
File Name RetroArch/bitmapfont.c
Method static void font_renderer_bmp_free(void *data)

```
....
224.     free(handle);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=453
Status	New

Calling free() (line 1449) on a variable that was not dynamically allocated (line 1449) in file RetroArch/btstack_hid.c may result with a crash.

	Source	Destination
File	RetroArch/btstack_hid.c	RetroArch/btstack_hid.c
Line	1461	1461
Object	hid	hid

Code Snippet

File Name	RetroArch/btstack_hid.c
Method	static void btstack_hid_free(const void *data)

```
....
1461.         free(hid);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=454
Status	New

Calling free() (line 1333) on a variable that was not dynamically allocated (line 1333) in file RetroArch/cdrom.c may result with a crash.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1419	1419
Object	buf	buf

Code Snippet	
File Name	RetroArch/cdrom.c
Method	struct string_list* cdrom_get_available_drives(void)

```
....
1419.             free(buf);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=455
Status	New

Calling free() (line 420) on a variable that was not dynamically allocated (line 420) in file RetroArch/config_file.c may result with a crash.

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	493	493
Object	line	line

Code Snippet	
File Name	RetroArch/config_file.c
Method	static int config_file_load_internal(

```
....
493.        free(line);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=456
Status	New

Calling free() (line 193) on a variable that was not dynamically allocated (line 193) in file RetroArch/drm_gfx.c may result with a crash.

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	204	204
Object	surface	surface

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_surface_free(void *data, struct drm_surface **sp)

```
....
204.     free(surface);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=457
Status	New

Calling free() (line 943) on a variable that was not dynamically allocated (line 943) in file RetroArch/drm_gfx.c may result with a crash.

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	962	962
Object	_drmvars	_drmvars

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_free(void *data)

```
....
962.      free(_drmvars);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=458
Status	New

Calling free() (line 554) on a variable that was not dynamically allocated (line 554) in file RetroArch/dtoverlay_main.c may result with a crash.

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	714	714
Object	paramv	paramv

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int dtoverlay_remove(STATE_T *state, const char *overlay, int and_later)

```
....
714.                    free(paramv);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=459
Status	New

Calling free() (line 1246) on a variable that was not dynamically allocated (line 1246) in file RetroArch/exynos_gfx.c may result with a crash.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	1270	1270
Object	pdata	pdata

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static void exynos_free(void *data)

```
....
1270.      free(pdata);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=460
Status	New

Calling free() (line 1246) on a variable that was not dynamically allocated (line 1246) in file RetroArch/exynos_gfx.c may result with a crash.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	1275	1275
Object	vid	vid

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static void exynos_free(void *data)

```
....
1275.      free(vid);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=461
Status	New

Calling free() (line 719) on a variable that was not dynamically allocated (line 719) in file RetroArch/flv_reader.c may result with a crash.

	Source	Destination
File	RetroArch/flv_reader.c	RetroArch/flv_reader.c
Line	730	730
Object	module	module

Code Snippet
File Name RetroArch/flv_reader.c
Method static VC_CONTAINER_STATUS_T flv_reader_close(VC_CONTAINER_T *p_ctx)

```
....
730.      free(module);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=462
Status	New

Calling free() (line 243) on a variable that was not dynamically allocated (line 243) in file RetroArch/hbl.c may result with a crash.

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c
Line	286	286
Object	buffer	buffer

Code Snippet
File Name RetroArch/hbl.c
Method int HBL_loadToMemory(const char *filepath, u32 args_size)

```
....
286.          free(buffer);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=463
Status	New

Calling free() (line 243) on a variable that was not dynamically allocated (line 243) in file RetroArch/hbl.c may result with a crash.

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c
Line	295	295
Object	buffer	buffer

Code Snippet
File Name RetroArch/hbl.c
Method int HBL_loadToMemory(const char *filepath, u32 args_size)

```
....
295.      free(buffer);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=464
Status	New

Calling free() (line 757) on a variable that was not dynamically allocated (line 757) in file RetroArch/rc_api_common.c may result with a crash.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	776	776
Object	chunk	chunk

Code Snippet
File Name RetroArch/rc_api_common.c
Method void rc_buf_destroy(rc_api_buffer_t* buffer) {

```
....
776.      free(chunk);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=465
Status	New

Calling free() (line 838) on a variable that was not dynamically allocated (line 838) in file RetroArch/shader_glsl.c may result with a crash.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	847	847
Object	glsl	glsl

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_deinit(void *data)

```
....
847.     free(glsl);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=466
Status	New

Calling free() (line 979) on a variable that was not dynamically allocated (line 979) in file RetroArch/shader_glsl.c may result with a crash.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1149	1149
Object	error_string	error_string

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void *gl_glsl_init(void *data, const char *path)

```
....
1149.        free(error_string);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=467
Status	New

Calling free() (line 127) on a variable that was not dynamically allocated (line 127) in file RetroArch/switch_nx_gfx.c may result with a crash.

	Source	Destination
File	RetroArch/switch_nx_gfx.c	RetroArch/switch_nx_gfx.c
Line	137	137
Object	font	font

Code Snippet
File Name RetroArch/switch_nx_gfx.c
Method static void switch_font_free(void *data, bool is_threaded)

```
....
137.     free(font);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=468
Status	New

Calling free() (line 819) on a variable that was not dynamically allocated (line 819) in file RetroArch/switch_nx_gfx.c may result with a crash.

	Source	Destination
File	RetroArch/switch_nx_gfx.c	RetroArch/switch_nx_gfx.c
Line	828	828
Object	sw	sw

Code Snippet
File Name RetroArch/switch_nx_gfx.c
Method static void switch_free(void *data)

```
....
828.     free(sw);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=469
Status	New

Calling free() (line 608) on a variable that was not dynamically allocated (line 608) in file RetroArch/upscale_256x_320x240.c may result with a crash.

	Source	Destination
File	RetroArch/upscale_256x_320x240.c	RetroArch/upscale_256x_320x240.c
Line	614	614
Object	filt	filt

Code Snippet
File Name RetroArch/upscale_256x_320x240.c
Method static void upscale_256x_320x240_generic_destroy(void *data)

```
....
614.      free(filt);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=470
Status	New

Calling free() (line 159) on a variable that was not dynamically allocated (line 159) in file RetroArch/wav_reader.c may result with a crash.

	Source	Destination
File	RetroArch/wav_reader.c	RetroArch/wav_reader.c
Line	166	166
Object	module	module

Code Snippet
File Name RetroArch/wav_reader.c
Method static VC_CONTAINER_STATUS_T wav_reader_close(VC_CONTAINER_T *p_ctx)

```
....
166.      free(module);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=471
Status	New

Calling free() (line 1116) on a variable that was not dynamically allocated (line 1116) in file RetroArch/xmb.c may result with a crash.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	1132	1132
Object	tmp	tmp

Code Snippet
File Name RetroArch/xmb.c
Method static char* xmb_path_dynamic_wallpaper(xmb_handle_t *xmb)

```
....
1132.         free(tmp);
```

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=1010010&projectid=10011&pathid=564
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1005 of RetroArch/xmb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	1051	1051
Object	AssignExpr	AssignExpr

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_render_messagebox_internal(

```
....
1051.      y                          = y_position - (list.size-1) *
line_height / 2;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=565
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 198 of RetroArch/hbl.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c
Line	225	225

Object	AssignExpr	AssignExpr

Code Snippet
File Name RetroArch/hbl.c
Method void log_rpx(const char *filepath, unsigned char *buf, size_t len)

```
....
225.        for (i = (LINE_LEN - (len % LINE_LEN)); i < LINE_LEN; i++)
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=566
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4944 of RetroArch/rgui.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	5090	5090
Object	AssignExpr	AssignExpr

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render(

```
....
5090.     bottom                    = (int)(entries_end - rgui-
>term_layout.height);
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=567
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3215 of RetroArch/ssl_srv.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/ssl_srv.c	RetroArch/ssl_srv.c
Line	3278	3278
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	RetroArch/ssl_srv.c
Method	

```
....
3278.                           ssl->conf->f_rng, ssl->conf->p_rng );
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=568
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 7458 of RetroArch/xmb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7482	7482
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	RetroArch/xmb.c
Method	static void xmb_list_insert(void *userdata,

```
....
7482.     current           = (int)selection;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=569
Status	New

A variable of a larger data type, y1, is being assigned to a smaller data type, in 4744 of RetroArch/xmb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	4841	4841
Object	y1	y1

Code Snippet	
File Name	RetroArch/xmb.c
Method	static void xmb_render(void *data,

```
....
4841.               int y1                  = (int)((y_curr -
half_entry_size) + 0.5f);
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=570
Status	New

A variable of a larger data type, y2, is being assigned to a smaller data type, in 4744 of RetroArch/xmb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	4842	4842
Object	y2	y2

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_render(void *data,

```
....
4842.               int y2                  = (int)((y_curr +
half_entry_size) + 0.5f);
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=571
Status	New

A variable of a larger data type, right_padding, is being assigned to a smaller data type, in 5194 of RetroArch/xmb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5406	5406
Object	right_padding	right_padding

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5406.           int right_padding = (thumbnail_box_width -
(int)right_thumbnail_draw_width) >> 1;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=572
Status	New

A variable of a larger data type, left_padding, is being assigned to a smaller data type, in 5194 of RetroArch/xmb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5405	5405
Object	left_padding	left_padding

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5405.           int left_padding  = (thumbnail_box_width -
(int)left_thumbnail_draw_width)  >> 1;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=573
Status	New

A variable of a larger data type, i, is being assigned to a smaller data type, in 7458 of RetroArch/xmb.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7467	7467
Object	i	i

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_list_insert(void *userdata,

```
....
7467.     int i                         = (int)list_size;
```

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=1010010&projectid=10011&pathid=421
Status	New

The application performs an illegal operation in exynos_setup_scale, in RetroArch/exynos_gfx.c. In line 846, the program attempts to divide by height, 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 height in exynos_setup_scale of RetroArch/exynos_gfx.c, at line 846.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	852	852
Object	height	height

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static void exynos_setup_scale(struct exynos_data *pdata,

```
....
852.     const float aspect = (float)width / (float)height;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=422
Status	New

The application performs an illegal operation in exynos_setup_scale, in RetroArch/exynos_gfx.c. In line 846, the program attempts to divide by aspect, 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 aspect in exynos_setup_scale of RetroArch/exynos_gfx.c, at line 846.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	875	875

Object	aspect	aspect

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static void exynos_setup_scale(struct exynos_data *pdata,

```
....
875.            h = (float)pdata->height * pdata->aspect / aspect;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=423
Status	New

The application performs an illegal operation in rgui_update_menu_viewport, in RetroArch/rgui.c. In line 5911, the program attempts to divide by desired_aspect, 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 desired_aspect in rgui_update_menu_viewport of RetroArch/rgui.c, at line 5911.

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	5957	5957
Object	desired_aspect	desired_aspect

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_update_menu_viewport(

```
....
5957.            delta = (device_aspect / desired_aspect - 1.0f) / 2.0f +
0.5f;
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=424
Status	New

The application performs an illegal operation in rc_buf_destroy, in RetroArch/rc_api_common.c. In line 757, the program attempts to divide by total, 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 in rc_buf_destroy of RetroArch/rc_api_common.c, at line 757.

	Source	Destination
File	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c

Line	782	782
Object	total	total

Code Snippet
File Name RetroArch/rc_api_common.c
Method void rc_buf_destroy(rc_api_buffer_t* buffer) {

```
....
782.            total - wasted, total, wasted, (float)(100.0 - (wasted *
100.0) / total));
```

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=1010010&projectid=10011&pathid=558
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1333 of RetroArch/cdrom.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1454	1454
Object	AssignExpr	AssignExpr

Code Snippet
File Name RetroArch/cdrom.c
Method struct string_list* cdrom_get_available_drives(void)

```
....
1454.        path[0]          += i;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=559
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1333 of RetroArch/cdrom.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1455	1455
Object	AssignExpr	AssignExpr

Code Snippet
File Name RetroArch/cdrom.c
Method struct string_list* cdrom_get_available_drives(void)

```
....
1455.         cdrom_path[8]     += i;
```

Char Overflow\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=560
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1076 of RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1089	1089
Object	AssignExpr	AssignExpr

Code Snippet
File Name RetroArch/test_x509.c
Method string_to_hash(const char *name)

```
....
1089.                     tmp[v ++] = c;
```

Char Overflow\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=561
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1114 of RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1127	1127
Object	AssignExpr	AssignExpr

Code Snippet
File Name RetroArch/test_x509.c
Method string_to_curve(const char *name)

```
....
1127.                    tmp[v ++] = c;
```

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=1010010&projectid=10011&pathid=917
Status New

Method xmb_list_push at line 7846 of RetroArch/xmb.c defines kiosk_mode_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to kiosk_mode_password, this variable is never cleared from memory.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7881	7881
Object	kiosk_mode_password	kiosk_mode_password

Code Snippet
File Name RetroArch/xmb.c
Method static int xmb_list_push(void *data, void *userdata,

```
....
7881.     const char *kiosk_mode_password = settings-
>paths.kiosk_mode_password;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=918
Status	New

Method menu_action_setting_disp_set_label_shader_num_passes at line 267 of RetroArch/menu_cbs_get_value.c defines pass_count, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass_count, this variable is never cleared from memory.

	Source	Destination
File	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	276	276
Object	pass_count	pass_count

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_shader_num_passes(

```
....
276.     unsigned pass_count         = shader ? shader->passes : 0;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=919
Status	New

Method gl_glsl_compile_programs at line 569 of RetroArch/shader_glsl.c defines pass, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pass, this variable is never cleared from memory.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	580	580
Object	pass	pass

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_compile_programs(

```
....
580.        struct video_shader_pass *pass = (struct video_shader_pass*)
```

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=1010010&projectid=10011&pathid=15
Status	New

The pointer br_aes_x86ni_ctrcbc_vtable at RetroArch/aes_x86ni_ctrcbc.c in line 32 is being used after it has been freed.

	Source	Destination
File	RetroArch/aes_x86ni_ctrcbc.c	RetroArch/aes_x86ni_ctrcbc.c
Line	34	34
Object	br_aes_x86ni_ctrcbc_vtable	br_aes_x86ni_ctrcbc_vtable

Code Snippet
File Name RetroArch/aes_x86ni_ctrcbc.c
Method br_aes_x86ni_ctrcbc_get_vtable(void)

```
....
34.   return br_aes_x86ni_supported() ? &br_aes_x86ni_ctrcbc_vtable :
NULL;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=16
Status	New

The pointer _end at RetroArch/hbl.c in line 83 is being used after it has been freed.

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c
Line	88	88
Object	_end	_end

Code Snippet

File Name	RetroArch/hbl.c
Method	void *getApplicationEndAddr(void)

```
....
88.     return _end;
```

Float Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Float Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Float Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=562
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 642 of RetroArch/retroarch.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	695	695
Object	AssignExpr	AssignExpr

Code Snippet

File Name	RetroArch/retroarch.c
Method	static void driver_adjust_system_rates(

```
....
695.            timing_skew_hz              = input_fps;
```

Float Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=563
Status	New

A variable of a larger data type, inp_sample_rate, is being assigned to a smaller data type, in 594 of RetroArch/retroarch.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	601	601
Object	inp_sample_rate	inp_sample_rate

Code Snippet
File Name RetroArch/retroarch.c
Method static float audio_driver_monitor_adjust_system_rates(

```
....
601.     float inp_sample_rate        = input_sample_rate;
```

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=1010010&projectid=10011&pathid=163
Status	New

The *config_file_extract_value method calls the strdup function, at line 208 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	239	239
Object	strdup	strdup

Code Snippet
File Name RetroArch/config_file.c
Method static char *config_file_extract_value(char *line)

```
....
239.             return strdup(value);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=100

	11&pathid=164
Status	New

The *config_file_extract_value method calls the strdup function, at line 208 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	255	255
Object	strdup	strdup

Code Snippet
File Name RetroArch/config_file.c
Method static char *config_file_extract_value(char *line)

```
....
255.            return strdup(value);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=165
Status	New

The config_set_double method calls the snprintf function, at line 1334 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	1338	1338
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_double(config_file_t *conf, const char *key, double val)

```
....
1338.     snprintf(buf, sizeof(buf), "%f", (float)val);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=166

Status	New

The config_set_float method calls the snprintf function, at line 1347 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	1350	1350
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_float(config_file_t *conf, const char *key, float val)

```
....
1350.     snprintf(buf, sizeof(buf), "%f", val);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=167
Status	New

The config_set_int method calls the snprintf function, at line 1354 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	1357	1357
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_int(config_file_t *conf, const char *key, int val)

```
....
1357.     snprintf(buf, sizeof(buf), "%d", val);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=168
Status	New

The config_set_uint method calls the snprintf function, at line 1361 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	1364	1364
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_uint(config_file_t *conf, const char *key, unsigned int val)

```
....
1364.     snprintf(buf, sizeof(buf), "%u", val);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=169
Status New

The config_set_hex method calls the snprintf function, at line 1368 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	1371	1371
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_hex(config_file_t *conf, const char *key, unsigned val)

```
....
1371.     snprintf(buf, sizeof(buf), "%x", val);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=170
Status New

The config_set_char method calls the snprintf function, at line 1382 of RetroArch/config_file.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	RetroArch/config_file.c	RetroArch/config_file.c
Line	1385	1385
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_set_char(config_file_t *conf, const char *key, char val)

```
....
1385.     snprintf(buf, sizeof(buf), "%c", val);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=171
Status New

The exynos_get_device_index method calls the snprintf function, at line 164 of RetroArch/exynos_gfx.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	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	175	175
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_get_device_index(void)

```
....
175.        snprintf(buf, sizeof(buf), "/dev/dri/card%d", index);
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=172
Status New

The exynos_open method calls the snprintf function, at line 522 of RetroArch/exynos_gfx.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	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	533	533
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_open(struct exynos_data *pdata)

```
....
533.        snprintf(buf, sizeof(buf), "/dev/dri/card%d", devidx);
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=173
Status New

The menu_action_setting_audio_mixer_stream_volume method calls the snprintf function, at line 92 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	107	107
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_audio_mixer_stream_volume(

```
....
107.     snprintf(s, len, "%.2f",
audio_driver_mixer_get_stream_volume(offset));
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=174
Status New

The menu_action_setting_disp_set_label_cheat_num_passes method calls the snprintf function, at line 113 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	123	123
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_cheat_num_passes(

```
....
123.     snprintf(s, len, "%u", cheat_manager_get_buf_size());
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=175
Status New

The menu_action_setting_disp_set_label_shader_num_passes method calls the snprintf function, at line 267 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	279	279
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_shader_num_passes(

```
....
279.     snprintf(s, len, "%u", pass_count);
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=176
Status New

The menu_action_setting_disp_set_label_shader_parameter_internal method calls the snprintf function, at line 318 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	333	333
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_shader_parameter_internal(

```
....
333.        snprintf(s, len, "%.2f [%.2f %.2f]",
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=177
Status New

The menu_action_setting_disp_set_label_shader_scale_pass method calls the snprintf function, at line 367 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	387	387
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_shader_scale_pass(

```
....
387.        snprintf(s, len, "%ux", scale_value);
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=178
Status New

The menu_action_setting_disp_set_label_cpu_policy method calls the snprintf function, at line 649 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	665	665
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_cpu_policy(

```
....
665.        snprintf(s2, len2, "%s %d [CPU(s) %s]", msg_hash_to_str(
```

Unchecked Return Value\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=179
Status New

The menu_action_setting_disp_set_label_cpu_policy method calls the snprintf function, at line 649 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	669	669
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_cpu_policy(

```
....
669.        snprintf(s2, len2, "%s %d", msg_hash_to_str(
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=180
Status New

The menu_action_cpu_managed_freq_label method calls the snprintf function, at line 673 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	716	716
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_cpu_managed_freq_label(

```
....
716.        snprintf(s, len, "%u MHz", freq / 1000);
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=181
Status New

The menu_action_cpu_freq_label method calls the snprintf function, at line 719 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	736	736
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_cpu_freq_label(

```
....
736.           snprintf(s, len, "%u MHz", d->min_policy_freq / 1000);
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=182
Status New

The menu_action_cpu_freq_label method calls the snprintf function, at line 719 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	741	741
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_cpu_freq_label(

```
....
741.            snprintf(s, len, "%u MHz", d->max_policy_freq / 1000);
```

Unchecked Return Value\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=183
Status New

The menu_action_setting_disp_set_label_cheat method calls the snprintf function, at line 927 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	940	940
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_cheat(

```
....
940.            snprintf(s, len, "(%s) : %s",
```

Unchecked Return Value\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=184
Status New

The menu_action_setting_disp_set_label_cheat method calls the snprintf function, at line 927 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	949	949
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_cheat(

```
....
949.            snprintf(s, len, "(%s) : %08X",
```

Unchecked Return Value\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=185
Status New

The menu_action_setting_disp_set_label_cheat_match method calls the snprintf function, at line 960 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	975	975
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_cheat_match(

```
....
975.     snprintf(s, len, "Prev: %u Curr: %u", prev_val, curr_val);
```

Unchecked Return Value\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=186
Status New

The menu_action_setting_disp_set_label_menu_disk_index method calls the snprintf function, at line 1140 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	1168	1168
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_menu_disk_index(

```
....
1168.         snprintf(s, len, "%u", current + 1);
```

Unchecked Return Value\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=187
Status New

The menu_action_setting_disp_set_label_menu_video_resolution method calls the snprintf function, at line 1171 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	1190	1190
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_menu_video_resolution(

```
....
1190.            snprintf(s, len,
msg_hash_to_str(MENU_ENUM_LABEL_VALUE_DONT_CARE));
```

Unchecked Return Value\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=188
Status New

The menu_action_setting_disp_set_label_menu_video_resolution method calls the snprintf function, at line 1171 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	1195	1195
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_menu_video_resolution(

```
....
1195.               snprintf(s, len,
msg_hash_to_str(MSG_SCREEN_RESOLUTION_FORMAT_DESC),
```

Unchecked Return Value\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=189
Status New

The menu_action_setting_disp_set_label_menu_video_resolution method calls the snprintf function, at line 1171 of RetroArch/menu_cbs_get_value.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	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	1198	1198
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_menu_video_resolution(

```
....
1198.               snprintf(s, len,
msg_hash_to_str(MSG_SCREEN_RESOLUTION_FORMAT_NO_DESC),
```

Unchecked Return Value\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=190
Status New

The *allocbuffer method calls the malloc function, at line 89 of RetroArch/models.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	RetroArch/models.c	RetroArch/models.c
Line	91	91
Object	malloc	malloc

Code Snippet
File Name RetroArch/models.c
Method static void *allocbuffer(int size)

```
....
91.     return malloc(size);
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=191
Status New

The *net_http_new method calls the snprintf function, at line 717 of RetroArch/net_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	RetroArch/net_http.c	RetroArch/net_http.c
Line	761	761
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
761.        snprintf(portstr, sizeof(portstr), ":%i", conn->port);
```

Unchecked Return Value\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=192
Status New

The rc_api_format_md5 method calls the snprintf function, at line 843 of RetroArch/rc_api_common.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	RetroArch/rc_api_common.c	RetroArch/rc_api_common.c
Line	844	844
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/rc_api_common.c
Method void rc_api_format_md5(char checksum[33], const unsigned char digest[16]) {

```
....
844.    snprintf(checksum, 33,
"%02x%02x%02x%02x%02x%02x%02x%02x%02x%02x%02x%02x%02x%02x%02x%02x",
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=193
Status New

The command_event method calls the snprintf function, at line 2197 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	2360	2360
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method bool command_event(enum event_command cmd, void *data)

```
....
2360.                    snprintf(msg, sizeof(msg),
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=194
Status New

The command_event method calls the snprintf function, at line 2197 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	2364	2364
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method bool command_event(enum event_command cmd, void *data)

```
....
2364.                    snprintf(msg, sizeof(msg),
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=195
Status New

The command_event method calls the snprintf function, at line 2197 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	2404	2404
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method bool command_event(enum event_command cmd, void *data)

```
....
2404.                  snprintf(msg, sizeof(msg),
msg_hash_to_str(MSG_PREEMPT_ENABLED),
```

Unchecked Return Value\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=196
Status New

The command_event method calls the snprintf function, at line 2197 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	2456	2456
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method bool command_event(enum event_command cmd, void *data)

```
....
2456.                        snprintf(msg, sizeof(msg),
```

Unchecked Return Value\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=197
Status New

The command_event method calls the snprintf function, at line 2197 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	2460	2460
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method bool command_event(enum event_command cmd, void *data)

```
....
2460.                        snprintf(msg, sizeof(msg),
msg_hash_to_str(MSG_SCREEN_RESOLUTION_NO_DESC),
```

Unchecked Return Value\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=198
Status New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	4995	4995
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
4995.      _PSUPP_BUF(buf, SUPPORTS_LIBRETRODB,      "LibretroDB",
"LibretroDB support");
```

Unchecked Return Value\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=199
Status New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	4996	4996
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
4996.      _PSUPP_BUF(buf, SUPPORTS_COMMAND,         "Command",
"Command interface support");
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=200
Status New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	4997	4997
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
4997.      _PSUPP_BUF(buf, SUPPORTS_NETWORK_COMMAND, "Network Command",
"Network Command interface support");
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=201
Status New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	4998	4998
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
4998.      _PSUPP_BUF(buf, SUPPORTS_SDL,              "SDL",
"SDL input/audio/video drivers");
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=202

Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	4999	4999
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
4999.      _PSUPP_BUF(buf, SUPPORTS_SDL2,            "SDL2",
"SDL2 input/audio/video drivers");
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=203
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5000	5000
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5000.      _PSUPP_BUF(buf, SUPPORTS_X11,             "X11",
"X11 input/video drivers");
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=100

	11&pathid=204
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5001	5001
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5001.      _PSUPP_BUF(buf, SUPPORTS_UDEV,            "UDEV",
"UDEV/EVDEV input driver");
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=205
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5002	5002
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5002.      _PSUPP_BUF(buf, SUPPORTS_WAYLAND,         "Wayland",
"Wayland input/video drivers");
```

Unchecked Return Value\Path 44:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=206
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5003	5003
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5003.      _PSUPP_BUF(buf, SUPPORTS_THREAD,          "Threads",
"Threading support");
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=207
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5004	5004
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5004.      _PSUPP_BUF(buf, SUPPORTS_VULKAN,          "Vulkan",
"Video driver");
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=208
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5005	5005
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5005.      _PSUPP_BUF(buf, SUPPORTS_METAL,           "Metal",
"Video driver");
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=209
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5006	5006
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5006.      _PSUPP_BUF(buf, SUPPORTS_OPENGL,          "OpenGL",
"Video driver");
```

Unchecked Return Value\Path 48:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=210
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5007	5007
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5007.      _PSUPP_BUF(buf, SUPPORTS_OPENGLES,        "OpenGLES",
"Video driver");
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=211
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5008	5008
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5008.      _PSUPP_BUF(buf, SUPPORTS_XVIDEO,          "XVideo",
"Video driver");
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=212
Status	New

The retroarch_print_features method calls the snprintf function, at line 4986 of RetroArch/retroarch.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	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5009	5009
Object	snprintf	snprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_features(void)

```
....
5009.     _PSUPP_BUF(buf, SUPPORTS_EGL,             "EGL",
"Video context driver");
```

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=1010010&projectid=10011&pathid=1322
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	1623	1623
Object	fgets	fgets

Code Snippet
File Name RetroArch/retroarch.c
Method struct string_list *string_list_new_special(enum string_list_type type,

```
....
1623.                 while (fgets(zone_desc, TIMEZONE_LENGTH,
zones_file))
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1323
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	651	651
Object	fgetc	fgetc

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1324
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	657	657
Object	fgetc	fgetc

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1325
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	1623	1623
Object	zone_desc	zone_desc

Code Snippet
File Name RetroArch/retroarch.c
Method struct string_list *string_list_new_special(enum string_list_type type,

```
....
1623.                   while (fgets(zone_desc, TIMEZONE_LENGTH,
zones_file))
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1326
Status	New

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	1030	1030
Object	status	status

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int overlay_applied(const char *overlay_dir)

```
....
1030.       bytes = fread(status, 1, sizeof(status), fp);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1327
Status	New

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c

Line	276	276
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/hbl.c
Method int HBL_loadToMemory(const char *filepath, u32 args_size)

```
....
276.        ret = fread(buffer + bytesRead, 1, blockSize, fp);
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1328
Status New

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	226	226
Object	line	line

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
226.     valid = fread(line, 1, sizeof(line)-1, fp);
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1329
Status New

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	318	318
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/models.c

Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
318.        valid += fread(line+valid, 1, sizeof(line)-1-valid, fp);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1330
Status	New

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	352	352
Object	m	m

Code Snippet

File Name	RetroArch/models.c
Method	static int load_wavefront_dat(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
352.     s = fread(m, 1, size, fp);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1331
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	311	311
Object	shader_data	shader_data

Code Snippet

File Name	RetroArch/shader_glsl.c
Method	static bool gl_glsl_load_binary_shader(GLuint shader, char *save_path)

```
....
311.        fread(shader_data, shader_size, 1, shader_binary);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1332
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	423	423
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/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 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1333
Status	New

	Source	Destination
File	RetroArch/midi_driver.c	RetroArch/midi_driver.c
Line	446	446
Object	Address	Address

Code Snippet
File Name RetroArch/midi_driver.c
Method bool midi_driver_read(uint8_t *byte)

```
....
446.         if (!midi_drv->read(rarch_midi_drv_data,
&rarch_midi_drv_input_event))
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1334
Status	New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1454	1454
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_dump(config_file_t *conf, FILE *file, bool sort)

```
....
1454.         fprintf(file, "#reference \"%s\"\n", ref_tmp->path);
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1335
Status New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1470	1470
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/config_file.c
Method void config_file_dump(config_file_t *conf, FILE *file, bool sort)

```
....
1470.           fprintf(file, "%s = \"%s\"\n", list->key, list->value);
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1336
Status New

	Source	Destination
File	RetroArch/config_file.c	RetroArch/config_file.c
Line	1482	1482
Object	fprintf	fprintf

Code Snippet

File Name	RetroArch/config_file.c
Method	void config_file_dump(config_file_t *conf, FILE *file, bool sort)

```
....
1482.         fprintf(file, "#include \"%s\"\n", includes->path);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1337
Status	New

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	174	174
Object	fprintf	fprintf

Code Snippet

File Name	RetroArch/dtoverlay_main.c
Method	int main(int argc, const char **argv)

```
....
174.             fprintf(stderr, "* unknown option '%s'\n", arg);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1338
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5054	5054
Object	fprintf	fprintf

Code Snippet

File Name	RetroArch/retroarch.c
Method	static void retroarch_print_version(void)

```
....
5054.      fprintf(stdout, "%s - %s\n",
```

Improper Resource Access Authorization\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1339
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5058	5058
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_version(void)

```
....
5058.     fprintf(stdout, "Version: %s", PACKAGE_VERSION);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1340
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5060	5060
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_version(void)

```
....
5060.     fprintf(stdout, " (Git %s)", retroarch_git_version);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1341
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c

Line	5062	5062
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_version(void)

```
....
5062.     fprintf(stdout, " " __DATE__ "\n");
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1342
Status New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5065	5065
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_version(void)

```
....
5065.     fprintf(stdout, "%s\n", str);
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1343
Status New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5085	5085
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_print_help(const char *arg0)

```
....
5085.     fprintf(stdout, "Usage: %s [OPTIONS]... [FILE]\n\n", arg0);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1344
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5661	5661
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static bool retroarch_parse_input_and_config(

```
....
5661.               fprintf(stderr, "%s\n",
msg_hash_to_str(MSG_ERROR_PARSING_ARGUMENTS));
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1345
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5662	5662
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static bool retroarch_parse_input_and_config(

```
....
5662.               fprintf(stderr, "Try '%s --help' for more
information\n", argv[0]);
```

Improper Resource Access Authorization\Path 25:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1346
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5737	5737
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static bool retroarch_parse_input_and_config(

```
....
5737.                  fprintf(stderr, "\n%s: unrecognized option
'%s'\n", argv[0], argv[optind]);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1347
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5739	5739
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/retroarch.c
Method static bool retroarch_parse_input_and_config(

```
....
5739.                  fprintf(stderr, "Try '%s --help' for more
information\n", argv[0]);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1348
Status	New

	Source	Destination

File	RetroArch/sslio.c	RetroArch/sslio.c
Line	271	271
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
271.                fprintf(stderr, "Algorithms:\n");
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1349
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	273	273
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
273.                fprintf(stderr, "   RNG:           %s\n", rngname);
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1350
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	275	275
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
275.                    fprintf(stderr, "   AES/CBC (enc): %s\n",
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1351
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	279	279
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
279.                    fprintf(stderr, "   AES/CBC (dec): %s\n",
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1352
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	283	283
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
283.                    fprintf(stderr, "   AES/CTR:       %s\n",
```

Improper Resource Access Authorization\Path 32:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1353
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	287	287
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
287.                    fprintf(stderr, "   AES/CCM:       %s\n",
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1354
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	291	291
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
291.                    fprintf(stderr, "   DES/CBC (enc): %s\n",
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1355
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	295	295

Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
295.                    fprintf(stderr, "   DES/CBC (dec): %s\n",
```

Improper Resource Access Authorization\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1356
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	299	299
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
299.                    fprintf(stderr, "   GHASH (GCM):   %s\n",
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1357
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	303	303
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
303.                    fprintf(stderr, "   ChaCha20:      %s\n",
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1358
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	307	307
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
307.                    fprintf(stderr, "   Poly1305:      %s\n",
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1359
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	311	311
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
311.                    fprintf(stderr, "   EC:            %s\n",
```

Improper Resource Access Authorization\Path 39:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1360
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	315	315
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
315.                    fprintf(stderr, "   ECDSA:          %s\n",
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1361
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	319	319
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
319.                    fprintf(stderr, "   RSA (vrfy):     %s\n",
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1362
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	350	350

Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
350.              fprintf(stderr, "ERROR: WSACreateEvent() failed with
%d\n",
```

Improper Resource Access Authorization\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1363
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	397	397
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
397.                                  fprintf(stderr,
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1364
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	403	403
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
403.                          fprintf(stderr, "ERROR: SSL error %d",
err);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1365
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	407	407
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
407.                               fprintf(stderr,
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1366
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	411	411
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
411.                               fprintf(stderr,
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1367
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	420	420
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
420.                                    fprintf(stderr, " (%s)\n", ename);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1368
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	438	438
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
438.                        fprintf(stderr, "Handshake completed\n");
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1369
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c

Line	439	439
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
439.                    fprintf(stderr, "   version:                ");
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1370
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	442	442
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
442.                            fprintf(stderr, "SSL 3.0");
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1371
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	445	445
Object	fprintf	fprintf

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
445.                            fprintf(stderr, "TLS 1.0");
```

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=1010010&projectid=10011&pathid=503
Status	New

The variable declared in null at RetroArch/dtoverlay_main.c in line 105 is not initialized when it is used by namelist at RetroArch/dtoverlay_main.c in line 1075.

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	113	1082
Object	null	namelist

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method int main(int argc, const char **argv)

```
....
113.      STATE_T *state = NULL;
```

File Name RetroArch/dtoverlay_main.c
Method static void free_state(STATE_T *state)

```
....
1082.      free(state->namelist);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=504
Status	New

The variable declared in null at RetroArch/exynos_gfx.c in line 820 is not initialized when it is used by clear at RetroArch/exynos_gfx.c in line 820.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	822	836
Object	null	clear

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static struct exynos_page *exynos_free_page(struct exynos_data *pdata)

```
....
822.     struct exynos_page *page = NULL;
....
836.     if (page->clear)
```

NULL Pointer Dereference\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=505
Status New

The variable declared in null at RetroArch/exynos_gfx.c in line 820 is not initialized when it is used by bo at RetroArch/exynos_gfx.c in line 820.

	Source	Destination
File	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	822	834
Object	null	bo

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static struct exynos_page *exynos_free_page(struct exynos_data *pdata)

```
....
822.     struct exynos_page *page = NULL;
....
834.     dst->bo[0] = page->bo->handle;
```

NULL Pointer Dereference\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=506
Status New

The variable declared in null at RetroArch/menu_cbs_get_value.c in line 282 is not initialized when it is used by source at RetroArch/menu_cbs_get_value.c in line 282.

	Source	Destination
File	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	291	295
Object	null	source

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_shader_pass(

```
....
291.     struct video_shader_pass *shader_pass = shader ? &shader-
>pass[type - MENU_SETTINGS_SHADER_PASS_0] : NULL;
....
295.        fill_pathname_base(s, shader_pass->source.path, len);
```

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=507
Status New

The variable declared in null at RetroArch/menu_cbs_get_value.c in line 282 is not initialized when it is used by source at RetroArch/menu_cbs_get_value.c in line 282.

	Source	Destination
File	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	291	294
Object	null	source

Code Snippet
File Name RetroArch/menu_cbs_get_value.c
Method static void menu_action_setting_disp_set_label_shader_pass(

```
....
291.     struct video_shader_pass *shader_pass = shader ? &shader-
>pass[type - MENU_SETTINGS_SHADER_PASS_0] : NULL;
....
294.     if (shader_pass && !string_is_empty(shader_pass->source.path))
```

NULL Pointer Dereference\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=100

	11&pathid=508
Status	New

The variable declared in null at RetroArch/net_http.c in line 689 is not initialized when it is used by useragentcopy at RetroArch/net_http.c in line 689.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	695	695
Object	null	useragentcopy

Code Snippet
File Name RetroArch/net_http.c
Method void net_http_connection_set_user_agent(

```
....
695.     conn->useragentcopy = user_agent ? strdup(user_agent) : NULL;
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=509
Status	New

The variable declared in null at RetroArch/net_http.c in line 698 is not initialized when it is used by headerscopy at RetroArch/net_http.c in line 698.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	704	704
Object	null	headerscopy

Code Snippet
File Name RetroArch/net_http.c
Method void net_http_connection_set_headers(

```
....
704.     conn->headerscopy = headers ? strdup(headers) : NULL;
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=510
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1323 is not initialized when it is used by name at RetroArch/test_x509.c in line 1442.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1331	1456
Object	null	name

Code Snippet
File Name RetroArch/test_x509.c
Method process_conf_file(const char *fname)

```
....
1331.       all_chains = NULL;
```

File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1456.       printf("%s: ", tc->name);
```

NULL Pointer Dereference\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=511
Status New

The variable declared in null at RetroArch/test_x509.c in line 1323 is not initialized when it is used by ee_key_name at RetroArch/test_x509.c in line 1442.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1331	1511
Object	null	ee_key_name

Code Snippet
File Name RetroArch/test_x509.c
Method process_conf_file(const char *fname)

```
....
1331.       all_chains = NULL;
```

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1511.       if (tc->ee_key_name == NULL) {
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=512
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1323 is not initialized when it is used by days at RetroArch/test_x509.c in line 1442.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1331	1541
Object	null	days

Code Snippet
File Name RetroArch/test_x509.c
Method process_conf_file(const char *fname)

```
....
1331.       all_chains = NULL;
```

File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1541.       br_x509_minimal_set_time(&ctx, tc->days, tc->seconds);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=513
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1323 is not initialized when it is used by seconds at RetroArch/test_x509.c in line 1442.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c

Line	1331	1541
Object	null	seconds

Code Snippet
File Name RetroArch/test_x509.c
Method process_conf_file(const char *fname)

```
....
1331.       all_chains = NULL;
```

File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1541.       br_x509_minimal_set_time(&ctx, tc->days, tc->seconds);
```

NULL Pointer Dereference\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=514
Status New

The variable declared in null at RetroArch/test_x509.c in line 1323 is not initialized when it is used by servername at RetroArch/test_x509.c in line 1442.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1331	1557
Object	null	servername

Code Snippet
File Name RetroArch/test_x509.c
Method process_conf_file(const char *fname)

```
....
1331.       all_chains = NULL;
```

File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1557.       ctx.vtable->start_chain(&ctx.vtable, tc->servername);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=515
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1512	1422
Object	null	key

Code Snippet

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1512.             ee_pkey_ref = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1422.                     pk2->key.rsa.n, pk2->key.rsa.nlen)
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=516
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1512	1422
Object	null	key

Code Snippet

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1512.             ee_pkey_ref = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1422.                   pk2->key.rsa.n, pk2->key.rsa.nlen)
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=517
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1512	1424
Object	null	key

Code Snippet

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1512.             ee_pkey_ref = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1424.                   pk2->key.rsa.e, pk2->key.rsa.elen);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=518
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1512	1424
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1512.             ee_pkey_ref = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1424.                   pk2->key.rsa.e, pk2->key.rsa.elen);
```

NULL Pointer Dereference\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=519
Status New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1512	1426
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1512.             ee_pkey_ref = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1426.             return pk1->key.ec.curve == pk2->key.ec.curve
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=520
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1512	1427
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1512.             ee_pkey_ref = NULL;
```

File Name RetroArch/test_x509.c
Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1427.                 && pk1->key.ec.qlen == pk2->key.ec.qlen
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=521
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c

Line	1512	1429
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1512.             ee_pkey_ref = NULL;
```

File Name RetroArch/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;
```

NULL Pointer Dereference\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=522
Status New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1421
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1421.             return eqbigint(pk1->key.rsa.n, pk1->key.rsa.nlen,
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=523
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1421
Object	null	key

Code Snippet

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1421.             return eqbigint(pk1->key.rsa.n, pk1->key.rsa.nlen,
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=524
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1423
Object	null	key

Code Snippet

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1423.                   && eqbigint(pk1->key.rsa.e, pk1->key.rsa.elen,
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=525
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1423
Object	null	key

Code Snippet

File Name RetroArch/test_x509.c

Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1423.                   && eqbigint(pk1->key.rsa.e, pk1->key.rsa.elen,
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=526
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1426
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1426.             return pk1->key.ec.curve == pk2->key.ec.curve
```

NULL Pointer Dereference\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=527
Status New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1427
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1427.                    && pk1->key.ec.qlen == pk2->key.ec.qlen
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=528
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1429
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/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;
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=529
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c

Line	1603	1428
Object	null	key

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1428.                     && memcmp(pk1->key.ec.q,
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=530
Status	New

The variable declared in null at RetroArch/test_x509.c in line 1442 is not initialized when it is used by key_type at RetroArch/test_x509.c in line 1408.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1603	1431
Object	null	key_type

Code Snippet
File Name RetroArch/test_x509.c
Method run_test_case(test_case *tc)

```
....
1603.             ee_pkey = NULL;
```

File Name RetroArch/test_x509.c

Method eqpkey(const br_x509_pkey *pk1, const br_x509_pkey *pk2)

```
....
1431.             fprintf(stderr, "unknown key type: %d\n", pk1-
>key_type);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=531
Status	New

The variable declared in null at RetroArch/xmb.c in line 7522 is not initialized when it is used by alt at RetroArch/xmb.c in line 7522.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7544	7544
Object	null	alt

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_list_deep_copy(const file_list_t *src, file_list_t *dst,

```
....
7544.         d->alt    = string_is_empty(d->alt)    ? NULL : strdup(d-
>alt);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=532
Status	New

The variable declared in null at RetroArch/xmb.c in line 7522 is not initialized when it is used by path at RetroArch/xmb.c in line 7522.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7545	7545
Object	null	path

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_list_deep_copy(const file_list_t *src, file_list_t *dst,

```
....
7545.         d->path   = string_is_empty(d->path)   ? NULL : strdup(d-
>path);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=533
Status	New

The variable declared in null at RetroArch/xmb.c in line 7522 is not initialized when it is used by label at RetroArch/xmb.c in line 7522.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	7546	7546
Object	null	label

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_list_deep_copy(const file_list_t *src, file_list_t *dst,

```
....
7546.         d->label = string_is_empty(d->label) ? NULL : strdup(d-
>label);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=534
Status	New

The variable declared in 0 at RetroArch/lgc.c in line 844 is not initialized when it is used by gcfinnum at RetroArch/lgc.c in line 844.

	Source	Destination
File	RetroArch/lgc.c	RetroArch/lgc.c
Line	850	850
Object	0	gcfinnum

Code Snippet
File Name RetroArch/lgc.c
Method static int runafewfinalizers (lua_State *L) {

```
....
850.     g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 33:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=535
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by bodytype at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	854
Object	state	bodytype

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
854.     state->bodytype    = T_FULL;
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=536
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by data at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	852
Object	state	data

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
852.     state->data        = NULL;
```

NULL Pointer Dereference\Path 35:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=537
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by part at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	853
Object	state	part

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
853.     state->part       = P_HEADER_TOP;
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=538
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by error at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	855
Object	state	error

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
855.     state->error      = false;
```

NULL Pointer Dereference\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=539
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by status at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	851
Object	state	status

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
851.     state->status     = -1;
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=540
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by pos at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	856
Object	state	pos

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
856.     state->pos        = 0;
```

NULL Pointer Dereference\Path 39:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=541
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by len at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	857
Object	state	len

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
857.     state->len        = 0;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=542
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by buflen at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	858
Object	state	buflen

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
858.     state->buflen     = 512;
```

NULL Pointer Dereference\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=543
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by data at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	860
Object	state	data

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
860.     if (!(state->data = (char*)malloc(state->buflen)))
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=544
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by sock_state at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	850
Object	state	sock_state

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
850.     state->sock_state = conn->sock_state;
```

NULL Pointer Dereference\Path 43:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=545
Status	New

The variable declared in state at RetroArch/net_http.c in line 717 is not initialized when it is used by buflen at RetroArch/net_http.c in line 717.

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	721	860
Object	state	buflen

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
721.     struct http_t *state  = NULL;
....
860.     if (!(state->data = (char*)malloc(state->buflen)))
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=546
Status	New

The variable declared in right_thumbnail at RetroArch/xmb.c in line 5194 is not initialized when it is used by status at RetroArch/xmb.c in line 5194.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5220	5290
Object	right_thumbnail	status

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5220.        gfx_thumbnail_t *right_thumbnail = NULL;
....
5290.                  right_thumbnail->status ==
GFX_THUMBNAIL_STATUS_AVAILABLE
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=547
Status	New

The variable declared in right_thumbnail at RetroArch/xmb.c in line 5194 is not initialized when it is used by status at RetroArch/xmb.c in line 5194.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5220	5291
Object	right_thumbnail	status

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5220.        gfx_thumbnail_t *right_thumbnail = NULL;
....
5291.                || right_thumbnail->status ==
GFX_THUMBNAIL_STATUS_PENDING);
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=548
Status	New

The variable declared in right_thumbnail at RetroArch/xmb.c in line 5194 is not initialized when it is used by status at RetroArch/xmb.c in line 5194.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5220	5316
Object	right_thumbnail	status

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5220.        gfx_thumbnail_t *right_thumbnail = NULL;
....
5316.              (right_thumbnail->status ==
GFX_THUMBNAIL_STATUS_MISSING &&
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=549
Status	New

The variable declared in left_thumbnail at RetroArch/xmb.c in line 5194 is not initialized when it is used by status at RetroArch/xmb.c in line 5194.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5221	5317
Object	left_thumbnail	status

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5221.        gfx_thumbnail_t *left_thumbnail  = NULL;
....
5317.               left_thumbnail->status  ==
GFX_THUMBNAIL_STATUS_MISSING))
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=550
Status	New

The variable declared in left_thumbnail at RetroArch/xmb.c in line 5194 is not initialized when it is used by status at RetroArch/xmb.c in line 5194.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5221	5293
Object	left_thumbnail	status

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5221.        gfx_thumbnail_t *left_thumbnail  = NULL;
....
5293.                  left_thumbnail->status  ==
GFX_THUMBNAIL_STATUS_AVAILABLE
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=551
Status	New

The variable declared in left_thumbnail at RetroArch/xmb.c in line 5194 is not initialized when it is used by status at RetroArch/xmb.c in line 5194.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5221	5294
Object	left_thumbnail	status

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_draw_fullscreen_thumbnails(

```
....
5221.        gfx_thumbnail_t *left_thumbnail  = NULL;
....
5294.               || left_thumbnail->status  ==
GFX_THUMBNAIL_STATUS_PENDING);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=552
Status	New

The variable declared in left_thumbnail at RetroArch/xmb.c in line 5194 is not initialized when it is used by status at RetroArch/xmb.c in line 5194.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	5221	5300
Object	left_thumbnail	status

Code Snippet

File Name	RetroArch/xmb.c
Method	static void xmb_draw_fullscreen_thumbnails(

```
....
5221.         gfx_thumbnail_t *left_thumbnail   = NULL;
....
5300.            show_left_thumbnail   = (left_thumbnail->status ==
GFX_THUMBNAIL_STATUS_AVAILABLE);
```

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=1010010&projectid=10011&pathid=594
Status	New

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	836	836
Object	n	n

Code Snippet

File Name	RetroArch/lstrlib.c
Method	static lua_Number adddigit (char *buff, int n, lua_Number x) {

```
....
836.     buff[n] = (d < 10 ? d + '0' : d - 10 + 'a');  /* add to buffer
*/
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=595
Status	New

	Source	Destination
File	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	861	861
Object	_len	_len

Code Snippet	
File Name	RetroArch/menu_cbs_get_value.c
Method	static void menu_action_setting_disp_set_label_input_desc(

```
....
861.              s[_len   ] = ' ';
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=596
Status	New

	Source	Destination
File	RetroArch/menu_cbs_get_value.c	RetroArch/menu_cbs_get_value.c
Line	867	867
Object	_len	_len

Code Snippet	
File Name	RetroArch/menu_cbs_get_value.c
Method	static void menu_action_setting_disp_set_label_input_desc(

```
....
867.              s[_len   ] = ' ';
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=597
Status	New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	420	420
Object	buf_pos	buf_pos

Code Snippet	
File Name	RetroArch/net_http.c
Method	void net_http_urlencode_full(char *dest,

```
....
420.     dest[buf_pos]    = '/';
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=598
Status	New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	639	639
Object	domain_len	domain_len

Code Snippet
File Name RetroArch/net_http.c
Method bool net_http_connection_done(struct http_connection_t *conn)

```
....
639.            urlcopy[domain_len] = '\0';
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=599
Status	New

	Source	Destination
File	RetroArch/net_http.c	RetroArch/net_http.c
Line	816	816
Object	len	len

Code Snippet
File Name RetroArch/net_http.c
Method struct http_t *net_http_new(struct http_connection_t *conn)

```
....
816.        len_str[len] = '\0';
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=600
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5419	5419
Object	_len	_len

Code Snippet
File Name RetroArch/retroarch.c
Method static void retroarch_parse_input_libretro_path(const char *path)

```
....
5419.            tmp_path[_len  ] = '_';
```

Unchecked Array Index\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=601
Status New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	6353	6353
Object	_len	_len

Code Snippet
File Name RetroArch/retroarch.c
Method bool retroarch_main_init(int argc, char *argv[])

```
....
6353.              str_output[_len  ] = '\n';
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=602
Status New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	3041	3041
Object	len	len

Code Snippet

File Name	RetroArch/rgui.c
Method	static void rgui_update_dynamic_theme_path(

```
....
3041.         rgui->theme_dynamic_path[len   ] = '.';
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=603
Status	New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	4666	4666
Object	_len	_len

Code Snippet

File Name	RetroArch/rgui.c
Method	static void rgui_render_osk(

```
....
4666.         msg[_len   ] = '\n';
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=604
Status	New

	Source	Destination
File	RetroArch/rgui.c	RetroArch/rgui.c
Line	7182	7182
Object	playlist_selection_ptr	playlist_selection_ptr

Code Snippet

File Name	RetroArch/rgui.c
Method	static void rgui_navigation_set(void *data, bool scroll)

```
....
7182.         rgui->playlist_selection[rgui->playlist_selection_ptr] =
selection;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=605
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1184	1184
Object	VIDEO_SHADER_STOCK_BLEND	VIDEO_SHADER_STOCK_BLEND

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void *gl_glsl_init(void *data, const char *path)

```
....
1184.        glsl->prg[VIDEO_SHADER_STOCK_BLEND] = glsl->prg[0];
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=606
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1185	1185
Object	VIDEO_SHADER_STOCK_BLEND	VIDEO_SHADER_STOCK_BLEND

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void *gl_glsl_init(void *data, const char *path)

```
....
1185.        glsl->uniforms[VIDEO_SHADER_STOCK_BLEND] = glsl-
>uniforms[0];
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=607
Status	New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	509	509
Object	u	u

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
509.                    pfd[u] = (HANDLE)fd_event;
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=608
Status New

	Source	Destination
File	RetroArch/sslio.c	RetroArch/sslio.c
Line	513	513
Object	u	u

Code Snippet
File Name RetroArch/sslio.c
Method run_ssl_engine(br_ssl_engine_context *cc, unsigned long fd, unsigned flags)

```
....
513.                        pfd[u] = h_in;
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=609
Status New

	Source	Destination
File	RetroArch/switch_nx_gfx.c	RetroArch/switch_nx_gfx.c
Line	467	467
Object	pos	pos

Code Snippet

File Name	RetroArch/switch_nx_gfx.c
Method	static void gfx_cpy_dsp_buf(uint32_t *buffer, uint32_t *image, int w, int h, uint32_t stride, bool blend)

```
....
467.                dest[pos] = pixel;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=610
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	2015	2015
Object	len	len

Code Snippet	
File Name	RetroArch/test_x509.c
Method	main(int argc, const char *argv[])

```
....
2015.                           dn[len] = 0;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=611
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	288	288
Object	v	v

Code Snippet	
File Name	RetroArch/test_x509.c
Method	HT_expand(HT *ht)

```
....
288.                    new_buckets[v] = e;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=612
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	330	330
Object	k	k

Code Snippet
File Name RetroArch/test_x509.c
Method HT_put(HT *ht, const char *name, void *value)

```
....
330.                ht->buckets[k] = e;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=613
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1007	1007
Object	ptr	ptr

Code Snippet
File Name RetroArch/test_x509.c
Method parse_hex(const char *name, long linenum, const char *value, size_t *len)

```
....
1007.                                buf[ptr] = (acc << 4) + c;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=614
Status	New

	Source	Destination

File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1060	1060
Object	ptr	ptr

Code Snippet
File Name RetroArch/test_x509.c
Method split_names(const char *value)

```
....
1060.                                   names[ptr] = name;
```

Unchecked Array Index\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=615
Status New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1069	1069
Object	ptr	ptr

Code Snippet
File Name RetroArch/test_x509.c
Method split_names(const char *value)

```
....
1069.                   names[ptr] = NULL;
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=616
Status New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	1135	1135
Object	len	len

Code Snippet
File Name RetroArch/xmb.c
Method static char* xmb_path_dynamic_wallpaper(xmb_handle_t *xmb)

```
....
1135.     path[len  ] = '.';
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=617
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	2473	2473
Object	len	len

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_context_reset_horizontal_list(

```
....
2473.           texturepath[len  ] = '.';
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=618
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	2485	2485
Object	len	len

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_context_reset_horizontal_list(

```
....
2485.                texturepath[len  ] = '.';
```

Unchecked Array Index\Path 26:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=619
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	2510	2510
Object	_len	_len

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_context_reset_horizontal_list(

```
....
2510.            sysname[_len    ] = '-';
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=620
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	6361	6361
Object	_len	_len

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_frame(void *data, video_frame_info_t *video_info)

```
....
6361.         msg[_len   ]                    = '\n';
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=621
Status	New

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	90	90

Object	EbtInt8	EbtInt8

Code Snippet
File Name RetroArch/Initialize.cpp
Method TBuiltIns::TBuiltIns()

```
....
90.      prefixes[EbtInt8]  = "i8";
```

Unchecked Array Index\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=622
Status New

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	91	91
Object	EbtUint8	EbtUint8

Code Snippet
File Name RetroArch/Initialize.cpp
Method TBuiltIns::TBuiltIns()

```
....
91.      prefixes[EbtUint8] = "u8";
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=623
Status New

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	92	92
Object	EbtInt16	EbtInt16

Code Snippet
File Name RetroArch/Initialize.cpp
Method TBuiltIns::TBuiltIns()

```
....
92.      prefixes[EbtInt16]   = "i16";
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=624
Status	New

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	93	93
Object	EbtUint16	EbtUint16

Code Snippet
File Name RetroArch/Initialize.cpp
Method TBuiltIns::TBuiltIns()

```
....
93.      prefixes[EbtUint16] = "u16";
```

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=1010010&projectid=10011&pathid=136
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1900	1900
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1900.                particle->a = (float)(rand() % fb_width);
```

Use of Insufficiently Random Values\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=137
Status New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1901	1901
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1901.                particle->b = (float)(rand() % fb_height);
```

Use of Insufficiently Random Values\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=138
Status New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1902	1902
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c

Method	static void rgui_init_particle_effect(

```
....
1902.                particle->c = (float)(rand() % 64 - 16) * 0.1f;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=139
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1903	1903
Object	rand	rand

Code Snippet	
File Name	RetroArch/rgui.c
Method	static void rgui_init_particle_effect(

```
....
1903.                particle->d = (float)(rand() % 64 - 48) * 0.1f;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=140
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1928	1928
Object	rand	rand

Code Snippet	
File Name	RetroArch/rgui.c
Method	static void rgui_init_particle_effect(

```
....
1928.                 particle->a = (float)(rand() % (fb_width / 3)) *
3.0f;
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=141
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1930	1930
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1930.                 particle->b = (float)(rand() % fb_height);
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=142
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1932	1932
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1932.                 particle->c = (float)weights[(unsigned)(rand() %
60)];
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=143
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1934	1934
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1934.                 particle->d = (particle->c / 12.0f) * (0.5f +
((float)(rand() % 150) / 200.0f));
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=144
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1948	1948
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1948.                 particle->a = 1.0f + (((float)rand() /
(float)RAND_MAX) * max_radius);
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=145
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1950	1950
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1950.                 particle->b = ((float)rand() / (float)RAND_MAX) *
2.0f * PI;
```

Use of Insufficiently Random Values\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=146
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1952	1952
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1952.                 particle->c = (float)((rand() % 100) + 1) *
0.001f;
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=147
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1954	1954
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1954.                 particle->d = (((float)((rand() % 50) + 1) /
200.0f) + 0.1f) * one_degree_radians;
```

Use of Insufficiently Random Values\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=148
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1965	1965
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1965.                 particle->a = (float)(rand() % fb_width);
```

Use of Insufficiently Random Values\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=149
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1967	1967
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1967.                 particle->b = (float)(rand() % fb_height);
```

Use of Insufficiently Random Values\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=150
Status	New

Method rgui_init_particle_effect at line 1883 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	1971	1971
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_init_particle_effect(

```
....
1971.                   particle->d = 1.0f + ((float)(rand() % 20) *
0.01f);
```

Use of Insufficiently Random Values\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=151
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2049	2049
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2049.                   particle->c    = particle->c + (float)(rand() % 16
- 9) * 0.01f;
```

Use of Insufficiently Random Values\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=152
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2050	2050
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2050.                 particle->d    = particle->d + (float)(rand() % 16
- 7) * 0.01f;
```

Use of Insufficiently Random Values\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=153
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2131	2131
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2131.                   particle->a = (float)(rand() % (fb_width / 3))
* 3.0f;
```

Use of Insufficiently Random Values\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=154
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2135	2135
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2135.                    particle->c = (float)weights[(unsigned)(rand()
% 60)];
```

Use of Insufficiently Random Values\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=155
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2137	2137
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2137.                    particle->d = (particle->c / 12.0f) * (0.5f +
((float)(rand() % 150) / 200.0f));
```

Use of Insufficiently Random Values\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=156
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2187	2187
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2187.                    particle->a = 1.0f + (((float)rand() /
(float)RAND_MAX) * max_radius);
```

Use of Insufficiently Random Values\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=157
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2189	2189
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2189.                    particle->b = ((float)rand() / (float)RAND_MAX)
* 2.0f * PI;
```

Use of Insufficiently Random Values\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=158
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2191	2191
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2191.                    particle->c = (float)((rand() % 100) + 1) *
0.001f;
```

Use of Insufficiently Random Values\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=159
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2193	2193
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2193.                    particle->d = (((float)((rand() % 50) + 1) /
200.0f) + 0.1f) * one_degree_radians;
```

Use of Insufficiently Random Values\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=160
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2240	2240
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2240.                    particle->a = (float)(rand() % fb_width);
```

Use of Insufficiently Random Values\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=161
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2242	2242
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2242.                    particle->b = (float)(rand() % fb_height);
```

Use of Insufficiently Random Values\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=162
Status	New

Method rgui_render_particle_effect at line 1981 of RetroArch/rgui.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	RetroArch/rgui.c	RetroArch/rgui.c
Line	2246	2246
Object	rand	rand

Code Snippet
File Name RetroArch/rgui.c
Method static void rgui_render_particle_effect(

```
....
2246.                    particle->d = 1.0f + ((float)(rand() % 20) *
0.01f);
```

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=1010010&projectid=10011&pathid=425
Status	New

The buffer allocated by <= in RetroArch/aes_x86ni_ctrcbc.c at line 457 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/aes_x86ni_ctrcbc.c	RetroArch/aes_x86ni_ctrcbc.c
Line	468	468
Object	<=	<=

Code Snippet
File Name RetroArch/aes_x86ni_ctrcbc.c
Method br_aes_x86ni_ctrcbc_decrypt(const br_aes_x86ni_ctrcbc_keys *ctx,

```
....
468.        for (u = 0; u <= num_rounds; u ++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=426
Status	New

The buffer allocated by <= in RetroArch/aes_x86ni_ctrcbc.c at line 51 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	RetroArch/aes_x86ni_ctrcbc.c	RetroArch/aes_x86ni_ctrcbc.c
Line	63	63
Object	<=	<=

Code Snippet
File Name RetroArch/aes_x86ni_ctrcbc.c
Method br_aes_x86ni_ctrcbc_ctr(const br_aes_x86ni_ctrcbc_keys *ctx,

```
....
63.    for (u = 0; u <= num_rounds; u ++) {
```

Potential Off by One Error in Loops\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=427
Status New

The buffer allocated by <= in RetroArch/aes_x86ni_ctrcbc.c at line 257 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/aes_x86ni_ctrcbc.c	RetroArch/aes_x86ni_ctrcbc.c
Line	268	268
Object	<=	<=

Code Snippet
File Name RetroArch/aes_x86ni_ctrcbc.c
Method br_aes_x86ni_ctrcbc_mac(const br_aes_x86ni_ctrcbc_keys *ctx,

```
....
268.        for (u = 0; u <= num_rounds; u ++) {
```

Potential Off by One Error in Loops\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=428
Status New

The buffer allocated by <= in RetroArch/aes_x86ni_ctrcbc.c at line 308 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/aes_x86ni_ctrcbc.c	RetroArch/aes_x86ni_ctrcbc.c
Line	320	320

Object	<=	<=

Code Snippet
File Name RetroArch/aes_x86ni_ctrcbc.c
Method br_aes_x86ni_ctrcbc_encrypt(const br_aes_x86ni_ctrcbc_keys *ctx,

```
....
320.         for (u = 0; u <= num_rounds; u ++) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=429
Status	New

The buffer allocated by <= in RetroArch/shader_glsl.c at line 979 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	1142	1142
Object	<=	<=

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void *gl_glsl_init(void *data, const char *path)

```
....
1142.      for (i = 0; i <= glsl->shader->passes; 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=1010010&projectid=10011&pathid=430
Status	New

The buffer allocated by <= in RetroArch/xmb.c at line 2084 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	2093	2093
Object	<=	<=

Code Snippet	
File Name	RetroArch/xmb.c
Method	static void xmb_list_switch_horizontal_list(xmb_handle_t *xmb)

```
....
2093.      for (j = 0; j <= list_size; j++)
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=431
Status	New

The buffer allocated by <= in RetroArch/xmb.c at line 2234 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	2240	2240
Object	<=	<=

Code Snippet	
File Name	RetroArch/xmb.c
Method	static void xmb_list_open_horizontal_list(xmb_handle_t *xmb)

```
....
2240.      for (j = 0; j <= list_size; j++)
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=432
Status	New

The buffer allocated by <= in RetroArch/xmb.c at line 2385 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	2391	2391
Object	<=	<=

Code Snippet	
File Name	RetroArch/xmb.c
Method	static void xmb_toggle_horizontal_list(xmb_handle_t *xmb)

```
....
2391.     for (i = 0; i <= list_size; i++)
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=433
Status	New

The buffer allocated by <= in RetroArch/xmb.c at line 5640 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	6203	6203
Object	<=	<=

Code Snippet
File Name RetroArch/xmb.c
Method static void xmb_frame(void *data, video_frame_info_t *video_info)

```
....
6203.         for (i = 0; i <= xmb_list_get_size(xmb,
MENU_LIST_HORIZONTAL)
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=434
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 5818 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	5833	5833
Object	<=	<=

Code Snippet
File Name RetroArch/Initialize.cpp
Method void TBuiltIns::add2ndGenerationSamplingImaging(int version, EProfile profile, const SpvVersion& spvVersion)

```
....
5833.      for (int image = 0; image <= 1; ++image) { // loop over
"bool" image vs sampler
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=435
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 5818 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	5835	5835
Object	<=	<=

Code Snippet
File Name RetroArch/Initialize.cpp
Method void TBuiltIns::add2ndGenerationSamplingImaging(int version, EProfile profile, const SpvVersion& spvVersion)

```
....
5835.          for (int shadow = 0; shadow <= 1; ++shadow) { // loop
over "bool" shadow or not
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=436
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 5818 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	5836	5836
Object	<=	<=

Code Snippet
File Name RetroArch/Initialize.cpp

Method	void TBuiltIns::add2ndGenerationSamplingImaging(int version, EProfile profile, const SpvVersion& spvVersion)

```
....
5836.              for (int ms = 0; ms <=1; ++ms) {
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=437
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 5818 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	5846	5846
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::add2ndGenerationSamplingImaging(int version, EProfile profile, const SpvVersion& spvVersion)

```
....
5846.                  for (int arrayed = 0; arrayed <= 1; ++arrayed) {
// loop over "bool" arrayed or not
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=438
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6201	6201
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp

Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6201.      for (int proj = 0; proj <= 1; ++proj) { // loop over "bool"
projective or not
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=439
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6206	6206
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6206.          for (int lod = 0; lod <= 1; ++lod) {
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=440
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6215	6215
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp

Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6215.              for (int bias = 0; bias <= 1; ++bias) {
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=441
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6224	6224
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6224.                  for (int offset = 0; offset <= 1; ++offset) { //
loop over "bool" offset or not
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=442
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6231	6231
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp

Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6231.                        for (int fetch = 0; fetch <= 1; ++fetch) { //
loop over "bool" fetch or not
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=443
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6242	6242
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6242.                            for (int grad = 0; grad <= 1; ++grad) {
// loop over "bool" grad or not
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=444
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6251	6251
Object	<=	<=

Code Snippet

File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6251.                                   for (int extraProj = 0; extraProj <=
1; ++extraProj) {
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=445
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6269	6269
Object	<=	<=

Code Snippet

File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6269.                                       for (int f16TexAddr = 0;
f16TexAddr <= 1; ++f16TexAddr) { // loop over 16-bit floating-point
texel addressing
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=446
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6278	6278
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6278.                                          for (int lodClamp = 0;
lodClamp <= 1 ;++lodClamp) { // loop over "bool" lod clamp
```

Potential Off by One Error in Loops\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=447
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6196 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6285	6285
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addSamplingFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6285.                                            for (int sparse = 0;
sparse <= 1; ++sparse) { // loop over "bool" sparse or not
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=448
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6514 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6532	6532
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addGatherFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6532.      for (int f16TexAddr = 0; f16TexAddr <= 1; ++f16TexAddr) { //
loop over 16-bit floating-point texel addressing
```

Potential Off by One Error in Loops\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=449
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6514 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6547	6547
Object	<=	<=

Code Snippet	
File Name	RetroArch/Initialize.cpp
Method	void TBuiltIns::addGatherFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6547.                  for (int sparse = 0; sparse <= 1; ++sparse) { //
loop over "bool" sparse or not
```

Potential Off by One Error in Loops\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=450
Status	New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6514 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6640	6640

Object	<=	<=

Code Snippet
File Name RetroArch/Initialize.cpp
Method void TBuiltIns::addGatherFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6640.              for (int f16TexAddr = 0; f16TexAddr <= 1;
++f16TexAddr) { // loop over 16-bit floating-point texel addressing
```

Potential Off by One Error in Loops\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=451
Status New

The buffer allocated by <= in RetroArch/Initialize.cpp at line 6514 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	RetroArch/Initialize.cpp	RetroArch/Initialize.cpp
Line	6655	6655
Object	<=	<=

Code Snippet
File Name RetroArch/Initialize.cpp
Method void TBuiltIns::addGatherFunctions(TSampler sampler, const TString& typeName, int version, EProfile profile)

```
....
6655.                          for (int sparse = 0; sparse <= 1;
++sparse) { // loop over "bool" sparse or not
```

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=1010010&projectid=10011&pathid=577
Status New

	Source	Destination
File	RetroArch/sha1.c	RetroArch/sha1.c

Line	279	279
Object	finalcount	sizeof

Code Snippet
File Name RetroArch/sha1.c
Method void SHA1Final(

```
....
279.      memset(&finalcount, '\0', sizeof(finalcount));
```

Sizeof Pointer Argument\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=578
Status New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	3837	3837
Object	tmp	sizeof

Code Snippet
File Name RetroArch/xmb.c
Method static int xmb_draw_item(

```
....
3837.        ticker_smooth.dst_str_len = sizeof(tmp);
```

Sizeof Pointer Argument\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=579
Status New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	4032	4032
Object	tmp	sizeof

Code Snippet
File Name RetroArch/xmb.c
Method static int xmb_draw_item(

```
....
4032.        ticker_smooth.dst_str_len = sizeof(tmp);
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=580
Status	New

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	1166	1166
Object	buf	sizeof

Code Snippet
File Name RetroArch/cdrom.c
Method int cdrom_get_inquiry(libretro_vfs_implementation_file *stream, char *model, int len, bool *is_cdrom)

```
....
1166.     int rv = cdrom_send_command(stream, DIRECTION_IN, buf,
sizeof(buf), cdb, sizeof(cdb), 0);
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=581
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	747	747
Object	frame_base	sizeof

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_find_uniforms(glsl_shader_data_t *glsl,

```
....
747.        snprintf(frame_base, sizeof(frame_base), "PassPrev%u",
pass);
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=582
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	753	753
Object	frame_base	sizeof

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_find_uniforms(glsl_shader_data_t *glsl,

```
....
753.        snprintf(frame_base, sizeof(frame_base), "Pass%u", i + 1);
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=583
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	756	756
Object	frame_base	sizeof

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_find_uniforms(glsl_shader_data_t *glsl,

```
....
756.        snprintf(frame_base, sizeof(frame_base), "PassPrev%u", pass
- (i + 1));
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=584
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	767	767
Object	frame_base	sizeof

Code Snippet
File Name RetroArch/shader_glsl.c
Method static void gl_glsl_find_uniforms(glsl_shader_data_t *glsl,

```
....
767.         snprintf(frame_base, sizeof(frame_base), "Prev%u", i);
```

Sizeof Pointer Argument\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=585
Status New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1090	1090
Object	tmp	sizeof

Code Snippet
File Name RetroArch/test_x509.c
Method string_to_hash(const char *name)

```
....
1090.                    if (v == sizeof tmp) {
```

Sizeof Pointer Argument\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=586
Status New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1128	1128
Object	tmp	sizeof

Code Snippet

File Name	RetroArch/test_x509.c
Method	string_to_curve(const char *name)

```
....
1128.                   if (v == sizeof tmp) {
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=587
Status	New

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	469	469
Object	Pointer	sizeof

Code Snippet	
File Name	RetroArch/cdrom.c
Method	static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
469.            for (j = 0; j < cmd_len / sizeof(*cmd); j++)
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=588
Status	New

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	485	485
Object	sense	sizeof

Code Snippet	
File Name	RetroArch/cdrom.c
Method	static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
485.        if (cached_read || !cdrom_send_command_linux(stream, dir,
xfer_buf_pos, request_len, cmd, cmd_len, sense, sizeof(sense)))
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=589
Status	New

	Source	Destination
File	RetroArch/cdrom.c	RetroArch/cdrom.c
Line	526	526
Object	sense	sizeof

Code Snippet
File Name RetroArch/cdrom.c
Method static int cdrom_send_command(libretro_vfs_implementation_file *stream, CDROM_CMD_Direction dir, void *buf, size_t len, unsigned char *cmd, size_t cmd_len, size_t skip)

```
....
526.           cdrom_print_sense_data(sense, sizeof(sense));
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=590
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	3931	3931
Object	entry_sublabel	sizeof

Code Snippet
File Name RetroArch/xmb.c
Method static int xmb_draw_item(

```
....
3931.              line_ticker_smooth.dst_str_len          =
sizeof(entry_sublabel);
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=591
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	3935	3935
Object	entry_sublabel_top_fade	sizeof

Code Snippet
File Name RetroArch/xmb.c
Method static int xmb_draw_item(

```
....
3935.              line_ticker_smooth.top_fade_str_len     =
sizeof(entry_sublabel_top_fade);
```

Sizeof Pointer Argument\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=592
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	3940	3940
Object	entry_sublabel_bottom_fade	sizeof

Code Snippet
File Name RetroArch/xmb.c
Method static int xmb_draw_item(

```
....
3940.              line_ticker_smooth.bottom_fade_str_len  =
sizeof(entry_sublabel_bottom_fade);
```

Sizeof Pointer Argument\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=593
Status	New

	Source	Destination
File	RetroArch/xmb.c	RetroArch/xmb.c
Line	3959	3959
Object	entry_sublabel	sizeof

Code Snippet
File Name RetroArch/xmb.c
Method static int xmb_draw_item(

```
....
3959.              line_ticker.len       = sizeof(entry_sublabel);
```

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=1010010&projectid=10011&pathid=1444
Status New

	Source	Destination
File	RetroArch/hbl.c	RetroArch/hbl.c
Line	252	252
Object	fp	fp

Code Snippet
File Name RetroArch/hbl.c
Method int HBL_loadToMemory(const char *filepath, u32 args_size)

```
....
252.     if (!(fp = fopen(filepath, "rb")))
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1445

Status	New

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	220	220
Object	fp	fp

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
220.     fp = fopen(modelname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1446
Status	New

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	350	350
Object	fp	fp

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_dat(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
350.     fp = fopen(modelname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1447
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	450	450

Object	f	f

Code Snippet
File Name RetroArch/test_x509.c
Method read_file(const char *name, size_t *len)

```
....
450.         f = fopen(name, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1448
Status New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	612	612
Object	conf	conf

Code Snippet
File Name RetroArch/test_x509.c
Method conf_init(const char *fname)

```
....
612.         conf = 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=1010010&projectid=10011&pathid=1449
Status New

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	1026	1026
Object	fp	fp

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int overlay_applied(const char *overlay_dir)

```
....
1026.       FILE *fp = fopen(status_path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1450
Status	New

	Source	Destination
File	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	300	300
Object	shader_binary	shader_binary

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_load_binary_shader(GLuint shader, char *save_path)

```
....
300.      FILE *shader_binary = fopen(save_path, "rb" );
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1451
Status	New

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	234	234
Object	mkdir	mkdir

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method int main(int argc, const char **argv)

```
....
234.        if (mkdir(work_dir, DIR_MODE) != 0)
```

Incorrect Permission Assignment For Critical Resources\Path 9:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1452
Status	New

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	248	248
Object	mkdir	mkdir

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method int main(int argc, const char **argv)

```
....
248.            if (mkdir(cfg_dir, DIR_MODE) != 0)
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1453
Status	New

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	988	988
Object	mkdir	mkdir

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int apply_overlay(const char *overlay_file, const char *overlay)

```
....
988.      else if (mkdir(overlay_dir, DIR_MODE) == 0)
```

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=1010010&projectid=10011&pathid=1454
Status	New

The overlay_applied method in RetroArch/dtoverlay_main.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	RetroArch/dtoverlay_main.c	RetroArch/dtoverlay_main.c
Line	1026	1026
Object	fopen	fopen

Code Snippet
File Name RetroArch/dtoverlay_main.c
Method static int overlay_applied(const char *overlay_dir)

```
....
1026.       FILE *fp = fopen(status_path, "r");
```

TOCTOU\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1455
Status New

The HBL_loadToMemory method in RetroArch/hbl.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	RetroArch/hbl.c	RetroArch/hbl.c
Line	252	252
Object	fopen	fopen

Code Snippet
File Name RetroArch/hbl.c
Method int HBL_loadToMemory(const char *filepath, u32 args_size)

```
....
252.      if (!(fp = fopen(filepath, "rb")))
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1456
Status New

The load_wavefront_obj method in RetroArch/models.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	RetroArch/models.c	RetroArch/models.c
Line	220	220
Object	fopen	fopen

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
220.     fp = fopen(modelname, "r");
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1457
Status New

The load_wavefront_dat method in RetroArch/models.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	RetroArch/models.c	RetroArch/models.c
Line	350	350
Object	fopen	fopen

Code Snippet
File Name RetroArch/models.c
Method static int load_wavefront_dat(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
350.     fp = fopen(modelname, "r");
```

TOCTOU\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1458
Status New

The gl_glsl_load_binary_shader method in RetroArch/shader_glsl.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	RetroArch/shader_glsl.c	RetroArch/shader_glsl.c
Line	300	300
Object	fopen	fopen

Code Snippet
File Name RetroArch/shader_glsl.c
Method static bool gl_glsl_load_binary_shader(GLuint shader, char *save_path)

```
....
300.     FILE *shader_binary = fopen(save_path, "rb" );
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1459
Status	New

The read_file method in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	450	450
Object	fopen	fopen

Code Snippet
File Name RetroArch/test_x509.c
Method read_file(const char *name, size_t *len)

```
....
450.         f = fopen(name, "rb");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1460
Status	New

The conf_init method in RetroArch/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	RetroArch/test_x509.c	RetroArch/test_x509.c

Line	612	612
Object	fopen	fopen

Code Snippet
File Name RetroArch/test_x509.c
Method conf_init(const char *fname)

```
....
612.        conf = fopen(fname, "r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1461
Status	New

The init_drm method in RetroArch/drm_gfx.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	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	603	603
Object	open	open

Code Snippet
File Name RetroArch/drm_gfx.c
Method static bool init_drm(void)

```
....
603.     drm.fd = open("/dev/dri/card0", O_RDWR);
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1462
Status	New

The exynos_get_device_index method in RetroArch/exynos_gfx.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	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	177	177

Object	open	open

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_get_device_index(void)

```
....
177.        fd = open(buf, O_RDWR);
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=1463
Status	New

The exynos_open method in RetroArch/exynos_gfx.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	RetroArch/exynos_gfx.c	RetroArch/exynos_gfx.c
Line	540	540
Object	open	open

Code Snippet
File Name RetroArch/exynos_gfx.c
Method static int exynos_open(struct exynos_data *pdata)

```
....
540.     fd = open(buf, O_RDWR);
```

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=1010010&projectid=10011&pathid=415
Status	New

	Source	Destination
File	RetroArch/drm_gfx.c	RetroArch/drm_gfx.c
Line	374	380
Object	format_str	sizeof

Code Snippet
File Name RetroArch/drm_gfx.c
Method static void drm_format_name(const unsigned int fourcc, char *format_str)

```
....
374.  static void drm_format_name(const unsigned int fourcc, char
*format_str)
....
380.                     strlcpy(format_str, format_info[i].name,
sizeof(format_str));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=416
Status	New

	Source	Destination
File	RetroArch/bitmapfont.c	RetroArch/bitmapfont.c
Line	68	68
Object	sizeof	sizeof

Code Snippet
File Name RetroArch/bitmapfont.c
Method bitmapfont_lut_t *bitmapfont_get_lut(void)

```
....
68.     font->lut = (bool**)calloc(1, BMP_ATLAS_SIZE * sizeof(bool*));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=417
Status	New

	Source	Destination
File	RetroArch/lgc.c	RetroArch/lgc.c
Line	493	493
Object	sizeof	sizeof

Code Snippet
File Name RetroArch/lgc.c
Method static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                            sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=418
Status	New

	Source	Destination
File	RetroArch/lgc.c	RetroArch/lgc.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet
File Name RetroArch/lgc.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=419
Status	New

	Source	Destination
File	RetroArch/lobject.c	RetroArch/lobject.c
Line	437	437
Object	sizeof	sizeof

Code Snippet
File Name RetroArch/lobject.c
Method const char *luaO_pushvfstring (lua_State *L, const char *fmt, va_list argp) {

```
....
437.          char buff[4*sizeof(void *) + 8]; /* should be enough space
for a '%p' */
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=420
Status	New

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	214	214
Object	sizeof	sizeof

Code Snippet
File Name RetroArch/test_x509.c
Method HT_new(void)

```
....
214.        ht->buckets = xmalloc(ht->num_buckets * sizeof(ht_elt *));
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=574
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	4889	4889
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/retroarch.c
Method void emscripten_mainloop(void)

```
....
4889.        if ((emscripten_frame_count % (black_frame_insertion+1)) !=
0)
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=575
Status	New

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	128	128
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
128.    else if (l + lsep < l || l + lsep > MAXSIZE / n)  /* may
overflow? */
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=576
Status	New

	Source	Destination
File	RetroArch/lstrlib.c	RetroArch/lstrlib.c
Line	1426	1426
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name RetroArch/lstrlib.c
Method static int str_packsize (lua_State *L) {

```
....
1426.      luaL_argcheck(L, totalsize <= MAXSIZE - size, 1,
```

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=1010010&projectid=10011&pathid=134

Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5647	5647
Object	getopt_long	getopt_long

Code Snippet
File Name RetroArch/retroarch.c
Method static bool retroarch_parse_input_and_config(

```
....
5647.           int c = getopt_long(argc, argv, optstring, opts, NULL);
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=135
Status	New

	Source	Destination
File	RetroArch/retroarch.c	RetroArch/retroarch.c
Line	5788	5788
Object	getopt_long	getopt_long

Code Snippet
File Name RetroArch/retroarch.c
Method static bool retroarch_parse_input_and_config(

```
....
5788.           int c = getopt_long(argc, argv, optstring, opts, NULL);
```

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=1010010&projectid=100

	11&pathid=553
Status	New

The size of the buffer used by xmalloc in len, at line 49 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	651	56
Object	fgetc	len

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name RetroArch/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=1010010&projectid=10011&pathid=554
Status	New

The size of the buffer used by xmalloc in len, at line 49 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	657	56
Object	fgetc	len

Code Snippet
File Name RetroArch/test_x509.c
Method conf_next_low(void)

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

File Name	RetroArch/test_x509.c
Method	xmalloc(size_t len)

```
....
56.   buf = malloc(len);
```

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=1010010&projectid=10011&pathid=555
Status	New

The size of the buffer used by load_wavefront_obj in "usemtl %s", at line 208 of RetroArch/models.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_wavefront_obj passes to "usemtl %s", at line 208 of RetroArch/models.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/models.c	RetroArch/models.c
Line	247	247
Object	"usemtl %s"	"usemtl %s"

Code Snippet

File Name	RetroArch/models.c
Method	static int load_wavefront_obj(const char *modelname, WAVEFRONT_MODEL_T *model, struct wavefront_model_loading_s *m)

```
....
247.           if (sscanf(s, "usemtl %s", /*MAX_MATERIAL_NAME-1,
*/model->material[m->num_materials].name) == 1) {
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1010010&projectid=10011&pathid=556
Status	New

The size of the buffer used by read_file in "%s/%s", at line 438 of RetroArch/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 RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	447	447
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name RetroArch/test_x509.c
Method read_file(const char *name, size_t *len)

```
....
447.        sprintf(dname, "%s/%s", DIRNAME, name);
```

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=1010010&projectid=10011&pathid=557
Status	New

The size of the buffer used by xmalloc in len, at line 49 of RetroArch/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 1985 of RetroArch/test_x509.c, to overwrite the target buffer.

	Source	Destination
File	RetroArch/test_x509.c	RetroArch/test_x509.c
Line	1985	56
Object	argv	len

Code Snippet
File Name RetroArch/test_x509.c
Method main(int argc, const char *argv[])

```
....
1985.  main(int argc, const char *argv[])
```

File Name	RetroArch/test_x509.c
Method	xmalloc(size_t len)

```
....
56.   buf = malloc(len);
```

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 boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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

CGI Stored XSS

Risk

What might happen

Stored malicious data might retrieve system information and exploit the system through CGI (Common Gateway Interface).

Cause

How does it happen

The CGI specification provides opportunities to read files, acquire shell access, and corrupt file systems on server machines and their attached hosts.

Means of gaining access include: exploiting assumptions of the script, exploiting weaknesses in the server environment, and exploiting weaknesses in other programs and system calls.

The primary weakness in CGI scripts is insufficient input validation.

General Recommendations

How to avoid it

Do not provide unnecessary file permissions.

Validate and encode all DB output.

Source Code Examples

Perl

Bad - Printing out data from BD without encoding

```
#!/usr/bin/perl
use CGI;
use DBI;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", @row),
      $cgi->end_html;
```

```
```

Good - Printing out from DB after encoding

```
#!/usr/bin/perl
use CGI;
use DBI;
use HTML::Entities;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", HTML::Entities::encode(@row)),
      $cgi->end_html;
```

Buffer Overflow OutOfBound

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

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;
}
```

Float 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

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

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 Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

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)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

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

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

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

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--;
       }
    }
}
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	6/19/2024
Common	0105849645654507	6/19/2024