demo Scan Report

Project Name	demo
Scan Start	Thursday, June 20, 2024 3:23:12 PM
Preset	Checkmarx Default
Scan Time	00h:01m:36s
Lines Of Code Scanned	4548
Files Scanned	3
Report Creation Time	Thursday, June 20, 2024 3:25:24 PM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1
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

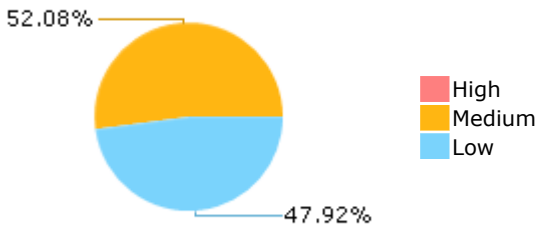
Results Limit

Results limit per query was set to 50

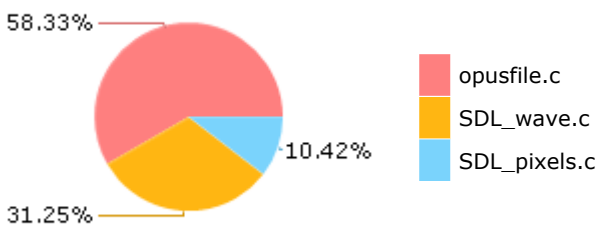
Selected Queries

Selected queries are listed in Result Summary

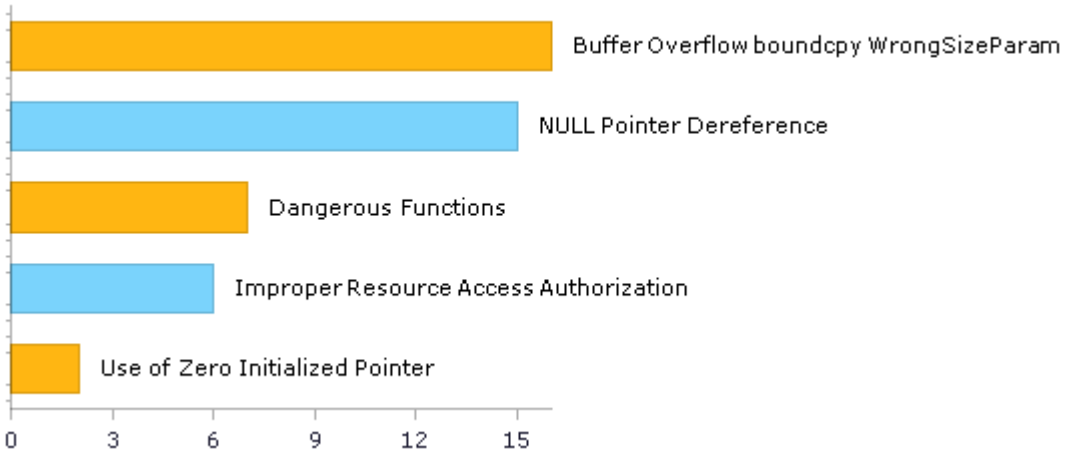
Result Summary



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	32	20
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	6	6
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
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	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	7	7
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	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	0	0
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	7	7
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	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	17	17
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	0	0
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	1	1
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	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.	6	6
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.	0	0
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.	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 - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	6	6
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)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	18	5
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	1	1
SI-11 Error Handling (P2)*	0	0
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	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 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

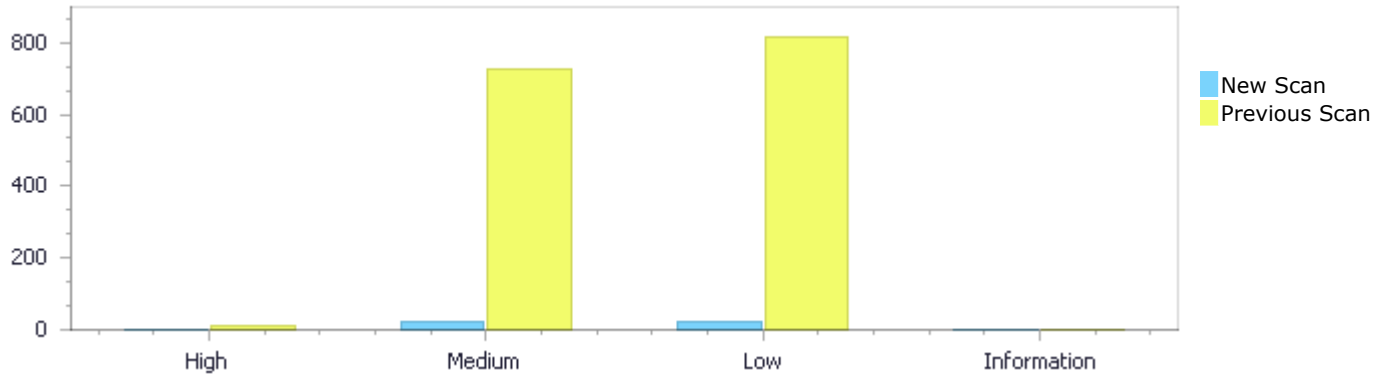
Scan Summary - Custom

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

Results Distribution By Status

Compared to project scan from 6/20/2024 12:17 AM

	High	Medium	Low	Information	Total
New Issues	0	25	23	0	48
Recurrent Issues	0	0	0	0	0
Total	0	25	23	0	48
Fixed Issues	12	724	817	0	1,553



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	0	25	23	0	48
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	25	23	0	48

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow boundcpy WrongSizeParam	16	Medium
Dangerous Functions	7	Medium
Use of Zero Initialized Pointer	2	Medium
NULL Pointer Dereference	15	Low
Improper Resource Access Authorization	6	Low

Arithmenic Operation On Boolean	1	Low
Heuristic 2nd Order Buffer Overflow read	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
opusfile.c	23
SDL_wave.c	2

Scan Results Details

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=1000008&projectid=1&pathid=1
Status	New

The size of the buffer used by op_make_decode_ready in channel_count, at line 1346 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_make_decode_ready passes to channel_count, at line 1346 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1375	1375
Object	channel_count	channel_count

Code Snippet
File Name opusfile.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1375.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=2
Status	New

The size of the buffer used by op_make_decode_ready in head, at line 1346 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_make_decode_ready passes to head, at line 1346 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c

Line	1375	1375
Object	head	head

Code Snippet
File Name opusfile.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1375.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=3
Status	New

The size of the buffer used by op_open_seekable2 in start_op_count, at line 1417 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to start_op_count, at line 1417 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1443	1443
Object	start_op_count	start_op_count

Code Snippet
File Name opusfile.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1443.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=4
Status	New

The size of the buffer used by op_open_seekable2 in op_start, at line 1417 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to op_start, at line 1417 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1443	1443

Object	op_start	op_start

Code Snippet
File Name opusfile.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1443.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=5
Status	New

The size of the buffer used by op_open_seekable2 in start_op_count, at line 1417 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to start_op_count, at line 1417 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1455	1455
Object	start_op_count	start_op_count

Code Snippet
File Name opusfile.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1455.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=6
Status	New

The size of the buffer used by op_open_seekable2 in _of, at line 1417 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open_seekable2 passes to _of, at line 1417 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1455	1455
Object	_of	_of

Code Snippet	
File Name	opusfile.c
Method	static int op_open_seekable2(OggOpusFile *_of){

```
....
1455.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=7
Status	New

The size of the buffer used by op_open1 in _initial_bytes, at line 1504 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open1 passes to _initial_bytes, at line 1504 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1530	1530
Object	_initial_bytes	_initial_bytes

Code Snippet	
File Name	opusfile.c
Method	static int op_open1(OggOpusFile *_of,

```
....
1530.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=8
Status	New

The size of the buffer used by op_open1 in buffer, at line 1504 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_open1 passes to buffer, at line 1504 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1530	1530
Object	buffer	buffer

Code Snippet	
File Name	opusfile.c

Method	static int op_open1(OggOpusFile *_of,

```
....
1530.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=9
Status	New

The size of the buffer used by op_stereo_filter in _nsamples, at line 3028 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_stereo_filter passes to _nsamples, at line 3028 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	3032	3032
Object	_nsamples	_nsamples

Code Snippet	
File Name	opusfile.c
Method	static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3032.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=10
Status	New

The size of the buffer used by op_stereo_filter in _src, at line 3028 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_stereo_filter passes to _src, at line 3028 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	3032	3032
Object	_src	_src

Code Snippet	
File Name	opusfile.c
Method	static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3032.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=11
Status	New

The size of the buffer used by op_read_native in nsamples, at line 2803 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_read_native passes to nsamples, at line 2803 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	2820	2820
Object	nsamples	nsamples

Code Snippet
File Name opusfile.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2820.           sizeof(*_pcm)*nchannels*nsamples);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=12
Status	New

The size of the buffer used by op_read_native in nchannels, at line 2803 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_read_native passes to nchannels, at line 2803 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	2820	2820
Object	nchannels	nchannels

Code Snippet
File Name opusfile.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2820.           sizeof(*_pcm)*nchannels*nsamples);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=13
Status	New

The size of the buffer used by op_read_native in _pcm, at line 2803 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_read_native passes to _pcm, at line 2803 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	2820	2820
Object	_pcm	_pcm

Code Snippet
File Name opusfile.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2820.           sizeof(*_pcm)*nchannels*nsamples);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=14
Status	New

The size of the buffer used by op_read_native in nchannels, at line 2803 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_read_native passes to nchannels, at line 2803 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	2888	2888
Object	nchannels	nchannels

Code Snippet
File Name opusfile.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2888.                   sizeof(*_pcm)*trimmed_duration*nchannels);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=15
Status	New

The size of the buffer used by op_read_native in trimmed_duration, at line 2803 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_read_native passes to trimmed_duration, at line 2803 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	2888	2888
Object	trimmed_duration	trimmed_duration

Code Snippet
File Name opusfile.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2888.                   sizeof(*_pcm)*trimmed_duration*nchannels);
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=16
Status	New

The size of the buffer used by op_read_native in _pcm, at line 2803 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_read_native passes to _pcm, at line 2803 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	2888	2888
Object	_pcm	_pcm

Code Snippet
File Name opusfile.c
Method static int op_read_native(OggOpusFile *_of,

```
....
2888.                   sizeof(*_pcm)*trimmed_duration*nchannels);
```

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=1000008&projectid=1&pathid=34
Status	New

The dangerous function, memcpy, was found in use at line 73 in opusfile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	opusfile.c	opusfile.c
Line	96	96
Object	memcpy	memcpy

Code Snippet
File Name opusfile.c
Method int op_test(OpusHead *_head,

```
....
96.      memcpy(data,_initial_data,_initial_bytes);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=35
Status	New

The dangerous function, memcpy, was found in use at line 1346 in opusfile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1375	1375

Object	memcpy	memcpy

Code Snippet
File Name opusfile.c
Method static int op_make_decode_ready(OggOpusFile *_of){

```
....
1375.      memcpy(_of->od_mapping,head->mapping,sizeof(*head-
>mapping)*channel_count);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=36
Status	New

The dangerous function, memcpy, was found in use at line 1417 in opusfile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1443	1443
Object	memcpy	memcpy

Code Snippet
File Name opusfile.c
Method static int op_open_seekable2(OggOpusFile *_of){

```
....
1443.    memcpy(op_start,_of->op,sizeof(*op_start)*start_op_count);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=37
Status	New

The dangerous function, memcpy, was found in use at line 1417 in opusfile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1455	1455
Object	memcpy	memcpy

Code Snippet	
File Name	opusfile.c
Method	static int op_open_seekable2(OggOpusFile *_of){

```
....
1455.    memcpy(_of->op,op_start,sizeof(*_of->op)*start_op_count);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=38
Status	New

The dangerous function, memcpy, was found in use at line 1504 in opusfile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	opusfile.c	opusfile.c
Line	1530	1530
Object	memcpy	memcpy

Code Snippet	
File Name	opusfile.c
Method	static int op_open1(OggOpusFile *_of,

```
....
1530.      memcpy(buffer,_initial_data,_initial_bytes*sizeof(*buffer));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=39
Status	New

The dangerous function, memcpy, was found in use at line 2803 in opusfile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	opusfile.c	opusfile.c
Line	2819	2819
Object	memcpy	memcpy

Code Snippet	
File Name	opusfile.c

Method	static int op_read_native(OggOpusFile *_of,

```
....
2819.          memcpy(_pcm,_of->od_buffer+nchannels*od_buffer_pos,
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=40
Status	New

The dangerous function, memcpy, was found in use at line 3028 in opusfile.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	opusfile.c	opusfile.c
Line	3032	3032
Object	memcpy	memcpy

Code Snippet	
File Name	opusfile.c
Method	static int op_stereo_filter(OggOpusFile *_of,void *_dst,int _dst_sz,

```
....
3032.    if(_nchannels==2)memcpy(_dst,_src,_nsamples*2*sizeof(*_src));
```

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=1000008&projectid=1&pathid=41
Status	New

The variable declared in data at SDL_wave.c in line 392 is not initialized when it is used by data at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	439	451

Object	data	data

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
439.                    chunk.data = NULL;
....
451.        format = (WaveFMT *)chunk.data;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=42
Status	New

The variable declared in data at SDL_wave.c in line 580 is not initialized when it is used by data at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	592	451
Object	data	data

Code Snippet
File Name SDL_wave.c
Method static int ReadChunk(SDL_RWops *src, Chunk *chunk)

```
....
592.              chunk->data = NULL;
```

File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
451.        format = (WaveFMT *)chunk.data;
```

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=1000008&projectid=1&pathid=17
Status	New

The variable declared in null at SDL_wave.c in line 392 is not initialized when it is used by index at SDL_wave.c in line 323.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	518	363
Object	null	index

Code Snippet

File Name SDL_wave.c

Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
518.         *audio_buf = NULL;
```

File Name SDL_wave.c

Method static int IMA_ADPCM_decode(Uint8 **audio_buf, Uint32 *audio_len)

```
....
363.                     state[c].index = *encoded++;
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=18
Status	New

The variable declared in null at SDL_wave.c in line 392 is not initialized when it is used by index at SDL_wave.c in line 323.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	522	363
Object	null	index

Code Snippet

File Name SDL_wave.c

Method	SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
522.                    *audio_buf = NULL;
```

File Name	SDL_wave.c
Method	static int IMA_ADPCM_decode(Uint8 **audio_buf, Uint32 *audio_len)

```
....
363.                    state[c].index = *encoded++;
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=19
Status	New

The variable declared in null at SDL_wave.c in line 392 is not initialized when it is used by hPredictor at SDL_wave.c in line 115.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	518	146
Object	null	hPredictor

Code Snippet	
File Name	SDL_wave.c
Method	SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
518.        *audio_buf = NULL;
```

File Name	SDL_wave.c
Method	static int MS_ADPCM_decode(Uint8 **audio_buf, Uint32 *audio_len)

```
....
146.                    state[1]->hPredictor = *encoded++;
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=20
Status	New

The variable declared in null at SDL_wave.c in line 392 is not initialized when it is used by hPredictor at SDL_wave.c in line 115.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	522	146
Object	null	hPredictor

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
522.                    *audio_buf = NULL;
```

File Name SDL_wave.c

Method static int MS_ADPCM_decode(Uint8 **audio_buf, Uint32 *audio_len)

```
....
146.                    state[1]->hPredictor = *encoded++;
```

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=21
Status New

The variable declared in null at SDL_wave.c in line 392 is not initialized when it is used by hPredictor at SDL_wave.c in line 115.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	518	144
Object	null	hPredictor

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
518.        *audio_buf = NULL;
```

File Name SDL_wave.c

Method	static int MS_ADPCM_decode(Uint8 **audio_buf, Uint32 *audio_len)

```
....
144.              state[0]->hPredictor = *encoded++;
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=22
Status	New

The variable declared in null at SDL_wave.c in line 392 is not initialized when it is used by hPredictor at SDL_wave.c in line 115.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	522	144
Object	null	hPredictor

Code Snippet	
File Name	SDL_wave.c
Method	SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
522.                    *audio_buf = NULL;
```

File Name	SDL_wave.c
Method	static int MS_ADPCM_decode(Uint8 **audio_buf, Uint32 *audio_len)

```
....
144.              state[0]->hPredictor = *encoded++;
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=23
Status	New

The variable declared in 0 at opusfile.c in line 630 is not initialized when it is used by op at opusfile.c in line 829.

	Source	Destination
File	opusfile.c	opusfile.c

Line	662	952
Object	0	op

Code Snippet
File Name opusfile.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
662.    return 0;
```

File Name opusfile.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
952.      prev_packet_gp=_of->op[pi].granulepos;
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=24
Status	New

The variable declared in 0 at opusfile.c in line 630 is not initialized when it is used by op at opusfile.c in line 829.

	Source	Destination
File	opusfile.c	opusfile.c
Line	662	950
Object	0	op

Code Snippet
File Name opusfile.c
Method static int op_granpos_add(ogg_int64_t *_dst_gp,ogg_int64_t _src_gp,

```
....
662.    return 0;
```

File Name opusfile.c

Method static int op_find_initial_pcm_offset(OggOpusFile *_of,

```
....
950.      OP_ALWAYS_TRUE(!op_granpos_add(&_of->op[pi].granulepos,
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=25
Status	New

The variable declared in format at SDL_wave.c in line 392 is not initialized when it is used by encoding at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	408	480
Object	format	encoding

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
408.        WaveFMT *format = NULL;
....
480.                                SDL_SwapLE16(format->encoding));
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=26
Status	New

The variable declared in format at SDL_wave.c in line 392 is not initialized when it is used by SDL_SwapLE16 at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	408	458
Object	format	SDL_SwapLE16

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
408.        WaveFMT *format = NULL;
....
458.        switch (SDL_SwapLE16(format->encoding)) {
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=27
Status	New

The variable declared in format at SDL_wave.c in line 392 is not initialized when it is used by encoding at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	408	485
Object	format	encoding

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
408.        WaveFMT *format = NULL;
....
485.                                SDL_SwapLE16(format->encoding));
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=28
Status	New

The variable declared in format at SDL_wave.c in line 392 is not initialized when it is used by frequency at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	408	490
Object	format	frequency

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
408.        WaveFMT *format = NULL;
....
490.        spec->freq = SDL_SwapLE32(format->frequency);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=29
Status	New

The variable declared in format at SDL_wave.c in line 392 is not initialized when it is used by SDL_SwapLE16 at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	408	491
Object	format	SDL_SwapLE16

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
408.         WaveFMT *format = NULL;
....
491.         switch (SDL_SwapLE16(format->bitspersample)) {
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=30
Status	New

The variable declared in format at SDL_wave.c in line 392 is not initialized when it is used by bitspersample at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	408	511
Object	format	bitspersample

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
408.         WaveFMT *format = NULL;
....
511.                     SDL_SwapLE16(format->bitspersample));
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=31
Status	New

The variable declared in format at SDL_wave.c in line 392 is not initialized when it is used by channels at SDL_wave.c in line 392.

	Source	Destination
File	SDL_wave.c	SDL_wave.c
Line	408	514
Object	format	channels

Code Snippet
File Name SDL_wave.c
Method SDL_AudioSpec * SDL_LoadWAV_RW (SDL_RWops *src, int freesrc,

```
....
408.         WaveFMT *format = NULL;
....
514.         spec->channels = (Uint8)SDL_SwapLE16(format->channels);
```

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=1000008&projectid=1&pathid=43
Status	New

	Source	Destination
File	opusfile.c	opusfile.c
Line	151	151
Object	buffer	buffer

Code Snippet
File Name opusfile.c

Method	static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=44
Status	New

	Source	Destination
File	SDL_pixels.c	SDL_pixels.c
Line	124	124
Object	fprintf	fprintf

Code Snippet	
File Name	SDL_pixels.c
Method	SDL_PixelFormat *SDL_AllocFormat(int bpp,

```
....
124.              fprintf(stderr,"bpp=%d ncolors=%d\n",bpp,ncolors);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=45
Status	New

	Source	Destination
File	SDL_pixels.c	SDL_pixels.c
Line	155	155
Object	fprintf	fprintf

Code Snippet	
File Name	SDL_pixels.c
Method	SDL_PixelFormat *SDL_AllocFormat(int bpp,

```
....
155.                  fprintf(stderr,"Rw=%d Rm=0x%02X\n",Rw,Rm);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=46
Status	New

	Source	Destination
File	SDL_pixels.c	SDL_pixels.c
Line	164	164
Object	fprintf	fprintf

Code Snippet
File Name SDL_pixels.c
Method SDL_PixelFormat *SDL_AllocFormat(int bpp,

```
....
164.                    fprintf(stderr,"Gw=%d Gm=0x%02X\n",Gw,Gm);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=47
Status	New

	Source	Destination
File	SDL_pixels.c	SDL_pixels.c
Line	173	173
Object	fprintf	fprintf

Code Snippet
File Name SDL_pixels.c
Method SDL_PixelFormat *SDL_AllocFormat(int bpp,

```
....
173.                    fprintf(stderr,"Bw=%d Bm=0x%02X\n",Bw,Bm);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=48
Status	New

	Source	Destination
File	SDL_pixels.c	SDL_pixels.c

Line	183	183
Object	fprintf	fprintf

Code Snippet
File Name SDL_pixels.c
Method SDL_PixelFormat *SDL_AllocFormat(int bpp,

```
....
183.                    fprintf(stderr,"Aw=%d Am=0x%02X\n",Aw,Am);
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read Version:0

Categories

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

Description
Heuristic 2nd Order Buffer Overflow read\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=1&pathid=32
Status	New

The size of the buffer used by op_get_data in _nbytes, at line 146 of opusfile.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that op_get_data passes to buffer, at line 146 of opusfile.c, to overwrite the target buffer.

	Source	Destination
File	opusfile.c	opusfile.c
Line	151	151
Object	buffer	_nbytes

Code Snippet
File Name opusfile.c
Method static int op_get_data(OggOpusFile *_of,int _nbytes){

```
....
151.    nbytes=(int)(*_of->callbacks.read)(_of->stream,buffer,_nbytes);
```

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=1000008&projectid=1&pathid=33
Status	New

	Source	Destination
File	opusfile.c	opusfile.c
Line	734	734
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name opusfile.c
Method static int op_granpos_cmp(ogg_int64_t _gp_a,ogg_int64_t _gp_b){

```
....
734.    return (_gp_a>_gp_b)-(_gp_b>_gp_a);
```

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

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));
    }
}
```

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;
}
```

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());
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Heuristic 2nd Order Buffer Overflow read

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	6/19/2024
Common	0105849645654507	6/19/2024