mobile-ffmpeg Scan Report

Project Name	mobile-ffmpeg
Scan Start	Saturday, June 22, 2024 1:58:13 AM
Preset	Checkmarx Default
Scan Time	02h:15m:29s
Lines Of Code Scanned	249598
Files Scanned	131
Report Creation Time	Saturday, June 22, 2024 9:04:01 AM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085
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

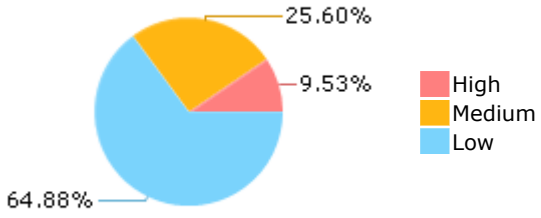
Results Limit

Results limit per query was set to 50

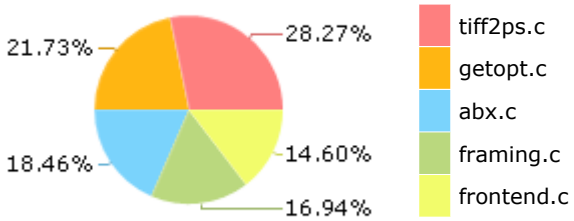
Selected Queries

Selected queries are listed in Result Summary

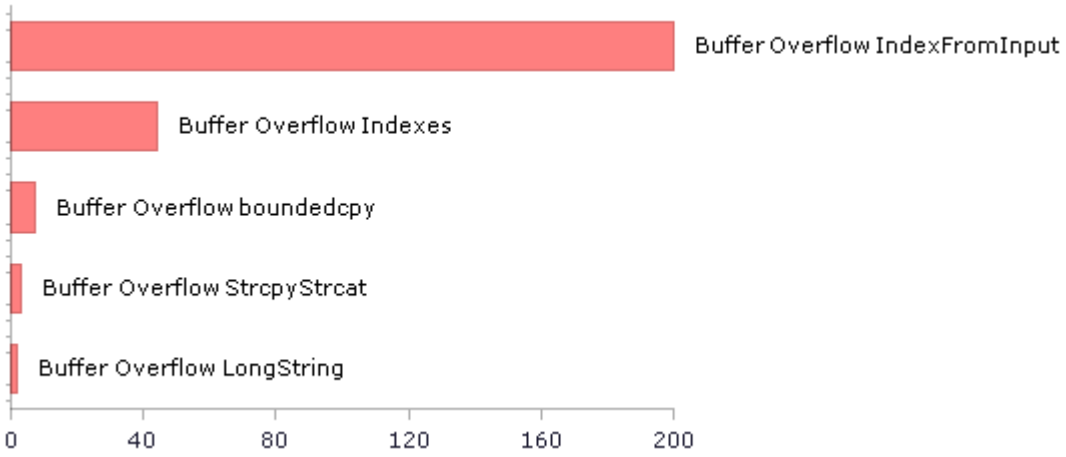
Result Summary



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	542	229
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	1108	1108
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	56	56
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	8	6
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	265	265
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	3	1
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	8	6
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	265	265
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	33	33
PCI DSS (3.2) - 6.5.2 - Buffer overflows	251	201
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.	21	21
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.	7	7
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.	21	19
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.	1089	1089
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.	52	52
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.	36	34

***** 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)	1129	1127
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)	2	2
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)	52	52
SC-4 Information in Shared Resources (P1)	1	1
SC-5 Denial of Service Protection (P1)*	211	78
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	245	193
SI-11 Error Handling (P2)*	97	97
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	33	33

***** 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

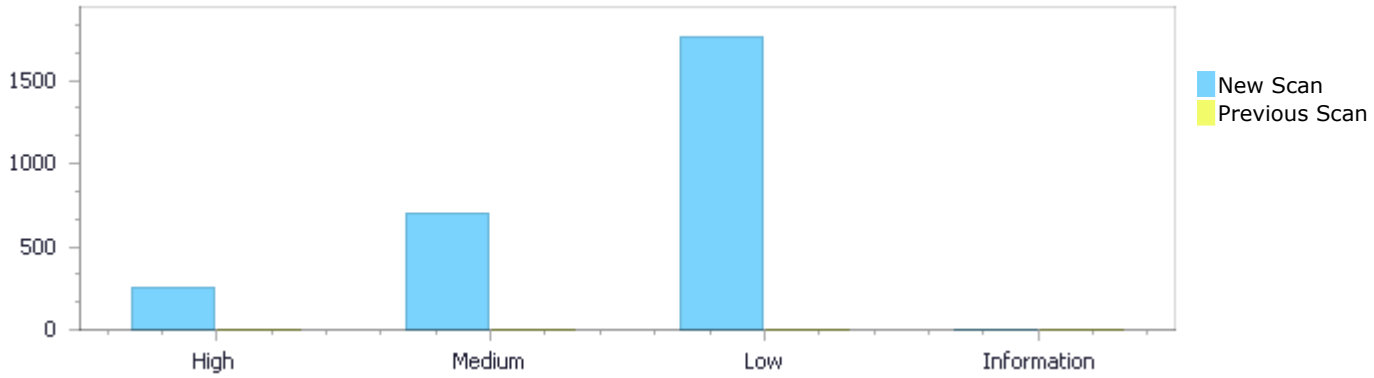
Scan Summary - Custom

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	259	696	1,764	0	2,719
Recurrent Issues	0	0	0	0	0
Total	259	696	1,764	0	2,719
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	259	696	1,764	0	2,719
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	259	696	1,764	0	2,719

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	200	High
Buffer Overflow Indexes	44	High
Buffer Overflow boundedcpy	7	High
Buffer Overflow StrcpyStrcat	3	High
Buffer Overflow LongString	2	High

String Termination Error	2	High
Format String Attack	1	High
Dangerous Functions	265	Medium
Buffer Overflow boundcpy WrongSizeParam	138	Medium
Divide By Zero	118	Medium
Use of Zero Initialized Pointer	75	Medium
Integer Overflow	25	Medium
Memory Leak	25	Medium
MemoryFree on StackVariable	11	Medium
Char Overflow	7	Medium
Use of Uninitialized Variable	6	Medium
Wrong Size t Allocation	6	Medium
Float Overflow	4	Medium
Short Overflow	4	Medium
Use of Uninitialized Pointer	4	Medium
Environment Injection	3	Medium
Use of Hard coded Cryptographic Key	2	Medium
Uncontrolled Recursion	1	Medium
Use After Free	1	Medium
Wrong Memory Allocation	1	Medium
Improper Resource Access Authorization	1087	Low
Sizeof Pointer Argument	149	Low
Unchecked Array Index	127	Low
Unchecked Return Value	97	Low
NULL Pointer Dereference	93	Low
Use of Insufficiently Random Values	52	Low
Potential Off by One Error in Loops	33	Low
TOCTOU	26	Low
Exposure of System Data to Unauthorized Control Sphere	21	Low
Incorrect Permission Assignment For Critical Resources	21	Low
Use of Sizeof On a Pointer Type	16	Low
Heuristic Buffer Overflow malloc	13	Low
Inconsistent Implementations	10	Low
Potential Path Traversal	8	Low
Arithmenic Operation On Boolean	7	Low
Heuristic 2nd Order Buffer Overflow malloc	1	Low
Insecure Temporary File	1	Low
Leaving Temporary Files	1	Low
Potential Precision Problem	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
mobile-ffmpeg/getopt.c	167
mobile-ffmpeg/framing.c	72
mobile-ffmpeg/abx.c	63
mobile-ffmpeg/dtls-stress.c	48
mobile-ffmpeg/makepng.c	38
mobile-ffmpeg/tiff2pdf.c	38

mobile-ffmpeg/DecUT_ParseSyntax.cpp	29
mobile-ffmpeg/rdppm.c	27
mobile-ffmpeg/adaptmap.c	27
mobile-ffmpeg/scale1.c	27

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=52
Status	New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.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 1207 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1207	997
Object	argv	i

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1207.  int  main ( int argc, char** argv )
```

File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
997.                    buff[i][0] = buff[i][1] = ((sample_t*)buff) [i];
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=53
Status	New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that readwave passes to buff, at line 947 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	995	997
Object	buff	i

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
995.              *len = fread ( buff, sizeof(sample_t), maxlen, fp );
....
997.                  buff[i][0] = buff[i][1] = ((sample_t*)buff) [i];
```

Buffer Overflow IndexFromInput\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=54
Status New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.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 1207 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1207	997
Object	argv	i

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1207.  int  main ( int argc, char** argv )
```

File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
997.                  buff[i][0] = buff[i][1] = ((sample_t*)buff) [i];
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=55
Status	New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that readwave passes to buff, at line 947 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	995	997
Object	buff	i

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
995.              *len = fread ( buff, sizeof(sample_t), maxlen, fp );
....
997.                  buff[i][0] = buff[i][1] = ((sample_t*)buff) [i];
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=56
Status	New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.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 1207 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1207	990
Object	argv	i

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1207.  int  main ( int argc, char** argv )
```

File Name mobile-ffmpeg/abx.c

Method	int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
990.                buff[i][0] = be16_le(buff[i][0]);
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=57
Status	New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that readwave passes to buff, at line 947 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	988	990
Object	buff	i

Code Snippet	
File Name	mobile-ffmpeg/abx.c
Method	int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
988.              *len = fread ( buff, sizeof(stereo_t), maxlen, fp );
....
990.               buff[i][0] = be16_le(buff[i][0]);
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=58
Status	New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.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 1207 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1207	991
Object	argv	i

Code Snippet	
File Name	mobile-ffmpeg/abx.c
Method	int main (int argc, char** argv)

```
....
1207.  int  main ( int argc, char** argv )
```

File Name mobile-ffmpeg/abx.c

Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
991.                buff[i][1] = be16_le(buff[i][1]);
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=59
Status	New

The size of the buffer used by readwave in i, at line 947 of mobile-ffmpeg/abx.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that readwave passes to buff, at line 947 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	988	991
Object	buff	i

Code Snippet

File Name mobile-ffmpeg/abx.c

Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
988.              *len = fread ( buff, sizeof(stereo_t), maxlen, fp );
....
991.               buff[i][1] = be16_le(buff[i][1]);
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=60
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c

Line	775	695
Object	argv	j

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c
Method int experiment (generator_t* const g,

```
....
695.                samples [j] [1] = ival;
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=61
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	684
Object	argv	j

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c
Method int experiment (generator_t* const g,

```
....
684.                samples [j] [0] = ival;
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=62
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	669
Object	argv	j

Code Snippet

File Name mobile-ffmpeg/ath.c

Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c

Method int experiment (generator_t* const g,

```
....
669.                samples [j] [0] = samples [j] [1] = ival;
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=63
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	669
Object	argv	j

Code Snippet

File Name mobile-ffmpeg/ath.c

Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c

Method int experiment (generator_t* const g,

```
....
669.                samples [j] [0] = samples [j] [1] = ival;
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=64
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	672
Object	argv	j

Code Snippet

File Name mobile-ffmpeg/ath.c

Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c

Method int experiment (generator_t* const g,

```
....
672.                samples [j] [0] = ival;
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=65
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	677
Object	argv	j

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c
Method int experiment (generator_t* const g,

```
....
677.              samples [j] [1] = ival;
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=66
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	681
Object	argv	j

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name	mobile-ffmpeg/ath.c
Method	int experiment (generator_t* const g,

```
....
681.                samples [j] [1] = +ival;
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=67
Status	New

The size of the buffer used by experiment in j, at line 636 of mobile-ffmpeg/ath.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 775 of mobile-ffmpeg/ath.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	680
Object	argv	j

Code Snippet	
File Name	mobile-ffmpeg/ath.c
Method	int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name	mobile-ffmpeg/ath.c
Method	int experiment (generator_t* const g,

```
....
680.                samples [j] [0] = ival == -32768 ? 32767 : -ival;
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=68
Status	New

The size of the buffer used by new_extension in dotpos, at line 54 of mobile-ffmpeg/frontend.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 704 of mobile-ffmpeg/frontend.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	704	84
Object	argv	dotpos

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method int main(int argc, char **argv)

```
....
704.  int main(int argc, char **argv)
```

File Name mobile-ffmpeg/frontend.c

Method static void new_extension(char *filename, char *extname, char *newname)

```
....
84.           newname[dotpos] = '\0';
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=69
Status	New

The size of the buffer used by shape_of in !=, at line 654 of mobile-ffmpeg/genpng.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 748 of mobile-ffmpeg/genpng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/genpng.c	mobile-ffmpeg/genpng.c
Line	748	660
Object	argv	!=

Code Snippet
File Name mobile-ffmpeg/genpng.c
Method main(int argc, const char **argv)

```
....
748.  main(int argc, const char **argv)
```

File Name mobile-ffmpeg/genpng.c

Method shape_of(const char *arg, double width, int f)

```
....
660.        shape_fn_ptr fn = shape_defs[i].function[width != 0][f];
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=70
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	260
Object	argc	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=71
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	260
Object	argv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=72
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	260
Object	getenv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=73

Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	260
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=74
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	260
Object	argv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=75
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	260
Object	getenv	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	_getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=76
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	259
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
259.              argv[middle + i] = tem;
```

Buffer Overflow IndexFromInput\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=77
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	259
Object	argv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
259.              argv[middle + i] = tem;
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=78
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	259
Object	getenv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
259.              argv[middle + i] = tem;
```

Buffer Overflow IndexFromInput\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=79
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	258
Object	argc	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	main (

```
....
1204.    int argc,
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
258.              argv[bottom + i] = argv[middle + i];
```

Buffer Overflow IndexFromInput\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=80
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	258
Object	argv	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	main (

```
....
1205.    char **argv
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
258.              argv[bottom + i] = argv[middle + i];
```

Buffer Overflow IndexFromInput\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=81

Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	258
Object	getenv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
258.              argv[bottom + i] = argv[middle + i];
```

Buffer Overflow IndexFromInput\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=82
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	243
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
243.              SWAP_FLAGS (bottom + i, top - (middle - bottom) + i);
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=83
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	243
Object	argv	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	main (

```
....
1205.    char **argv
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
243.              SWAP_FLAGS (bottom + i, top - (middle - bottom) + i);
```

Buffer Overflow IndexFromInput\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=84
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	243
Object	getenv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
243.              SWAP_FLAGS (bottom + i, top - (middle - bottom) + i);
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=85
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	243
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
243.              SWAP_FLAGS (bottom + i, top - (middle - bottom) + i);
```

Buffer Overflow IndexFromInput\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=86
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	243
Object	argv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
243.              SWAP_FLAGS (bottom + i, top - (middle - bottom) + i);
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=87
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	243
Object	getenv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
243.              SWAP_FLAGS (bottom + i, top - (middle - bottom) + i);
```

Buffer Overflow IndexFromInput\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=88
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	241
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
241.              argv[bottom + i] = argv[top - (middle - bottom) + i];
```

Buffer Overflow IndexFromInput\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=89

Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	241
Object	argv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
241.              argv[bottom + i] = argv[top - (middle - bottom) + i];
```

Buffer Overflow IndexFromInput\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=90
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	241
Object	getenv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
241.              argv[bottom + i] = argv[top - (middle - bottom) + i];
```

Buffer Overflow IndexFromInput\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=91
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	240
Object	argc	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	main (

```
....
1204.    int argc,
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
240.              tem = argv[bottom + i];
```

Buffer Overflow IndexFromInput\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=92
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	240
Object	argv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
240.              tem = argv[bottom + i];
```

Buffer Overflow IndexFromInput\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=93
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	240
Object	getenv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
240.              tem = argv[bottom + i];
```

Buffer Overflow IndexFromInput\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=94
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	260
Object	argc	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=95
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	260
Object	argv	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	main (

```
....
1205.    char **argv
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=96
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	260
Object	getenv	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	_getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=97

Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	260
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=98
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	260
Object	argv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=99
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	260
Object	getenv	BinaryExpr

Code Snippet

File Name	mobile-ffmpeg/getopt.c
Method	_getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name	mobile-ffmpeg/getopt.c
Method	exchange (

```
....
260.              SWAP_FLAGS (bottom + i, middle + i);
```

Buffer Overflow IndexFromInput\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=100
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	258
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
258.              argv[bottom + i] = argv[middle + i];
```

Buffer Overflow IndexFromInput\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=101
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	258
Object	argv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
258.              argv[bottom + i] = argv[middle + i];
```

Buffer Overflow Indexes

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

Categories

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

Description

Buffer Overflow Indexes\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1
Status	New

The size of the buffer used by get_text_gray_row in read_pbm_integer, at line 146 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	158
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
158.        *ptr++ = rescale[read_pbm_integer(cinfo, infile, maxval)];
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	201
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=3
Status New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	198
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.        GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=4
Status	New

The size of the buffer used by get_text_gray_cmyk_row in read_pbm_integer, at line 208 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	228
Object	getc	read_pbm_integer

Code Snippet

File Name mobile-ffmpeg/rdppm.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
228.        JSAMPLE gray = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=5
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=6
Status New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=7
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	275
Object	getc	read_pbm_integer

Code Snippet

File Name mobile-ffmpeg/rdppm.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=8
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 9:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=9
Status New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=10
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	272
Object	getc	read_pbm_integer

Code Snippet

File Name mobile-ffmpeg/rdppm.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=11
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	304
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
304.        JSAMPLE r = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 12:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=12
Status New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	305
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
305.        JSAMPLE g = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=13
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	91	306
Object	getc	read_pbm_integer

Code Snippet

File Name mobile-ffmpeg/rdppm.c

Method pbm_getc(FILE *infile)

```
....
91.     ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
306.        JSAMPLE b = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=14
Status	New

The size of the buffer used by get_text_gray_row in read_pbm_integer, at line 146 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	158
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_gray_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
158.       *ptr++ = rescale[read_pbm_integer(cinfo, infile, maxval)];
```

Buffer Overflow Indexes\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=15
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	201
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name	mobile-ffmpeg/rdppm.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
201.         GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=16
Status	New

The size of the buffer used by get_text_gray_rgb_row in read_pbm_integer, at line 173 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	198
Object	getc	read_pbm_integer

Code Snippet

File Name	mobile-ffmpeg/rdppm.c
Method	pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name	mobile-ffmpeg/rdppm.c
Method	get_text_gray_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
198.         GRAY_RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=17
Status	New

The size of the buffer used by get_text_gray_cmyk_row in read_pbm_integer, at line 208 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	228
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_gray_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
228.         JSAMPLE gray = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=18
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=19
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet

File Name	mobile-ffmpeg/rdppm.c
Method	pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name	mobile-ffmpeg/rdppm.c
Method	get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=20
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	275
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
275.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],)
```

Buffer Overflow Indexes\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=21
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	272
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=22
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	272
Object	getc	read_pbm_integer

Code Snippet

File Name mobile-ffmpeg/rdppm.c

Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.        RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=23
Status	New

The size of the buffer used by get_text_rgb_row in read_pbm_integer, at line 248 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	272
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_rgb_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
272.         RGB_READ_LOOP(rescale[read_pbm_integer(cinfo, infile,
maxval)],
```

Buffer Overflow Indexes\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=24
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	304
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
304.        JSAMPLE r = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=25
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	305
Object	getc	read_pbm_integer

Code Snippet

File Name mobile-ffmpeg/rdppm.c

Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c

Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
305.        JSAMPLE g = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=26
Status	New

The size of the buffer used by get_text_rgb_cmyk_row in read_pbm_integer, at line 282 of mobile-ffmpeg/rdppm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that pbm_getc passes to getc, at line 85 of mobile-ffmpeg/rdppm.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	94	306
Object	getc	read_pbm_integer

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method pbm_getc(FILE *infile)

```
....
94.         ch = getc(infile);
```

File Name mobile-ffmpeg/rdppm.c
Method get_text_rgb_cmyk_row(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
306.         JSAMPLE b = rescale[read_pbm_integer(cinfo, infile,
maxval)];
```

Buffer Overflow Indexes\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=27
Status	New

The size of the buffer used by new_extension in dotpos, at line 54 of mobile-ffmpeg/frontend.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 704 of mobile-ffmpeg/frontend.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	704	84
Object	argv	dotpos

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method int main(int argc, char **argv)

```
....
704.  int main(int argc, char **argv)
```

File Name mobile-ffmpeg/frontend.c
Method static void new_extension(char *filename, char *extname, char *newname)

```
....
84.           newname[dotpos] = '\0';
```

Buffer Overflow Indexes\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=28
Status	New

The size of the buffer used by shape_of in width, at line 654 of mobile-ffmpeg/genpng.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 748 of mobile-ffmpeg/genpng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/genpng.c	mobile-ffmpeg/genpng.c
Line	748	660
Object	argv	width

Code Snippet
File Name mobile-ffmpeg/genpng.c
Method main(int argc, const char **argv)

```
....
748.  main(int argc, const char **argv)
```

File Name mobile-ffmpeg/genpng.c
Method shape_of(const char *arg, double width, int f)

```
....
660.        shape_fn_ptr fn = shape_defs[i].function[width != 0][f];
```

Buffer Overflow Indexes\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=29
Status	New

The size of the buffer used by main in code, at line 38 of mobile-ffmpeg/latticetune.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 38 of mobile-ffmpeg/latticetune.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	38	122

Object	argv	code

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
38.  int main(int argc,char *argv[]){
....
122.          hits[code]+=val;
```

Buffer Overflow Indexes\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=30
Status	New

The size of the buffer used by main in index, at line 38 of mobile-ffmpeg/latticetune.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 38 of mobile-ffmpeg/latticetune.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	38	149
Object	argv	index

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
38.  int main(int argc,char *argv[]){
....
149.            fprintf(stderr,"%+3.1f,", c-
>quantlist[index]*_float32_unpack(c->q_delta)+
```

Buffer Overflow Indexes\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=31
Status	New

The size of the buffer used by set_color in blue, at line 238 of mobile-ffmpeg/makepng.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 1678 of mobile-ffmpeg/makepng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c

Line	1678	244
Object	argv	blue

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1678.  main(int argc, char **argv)
```

File Name mobile-ffmpeg/makepng.c

Method set_color(png_colorp color, png_bytep trans, unsigned int red,

```
....
244.      color->blue = gamma_table[blue];
```

Buffer Overflow Indexes\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=32
Status	New

The size of the buffer used by set_color in green, at line 238 of mobile-ffmpeg/makepng.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 1678 of mobile-ffmpeg/makepng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1678	243
Object	argv	green

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1678.  main(int argc, char **argv)
```

File Name mobile-ffmpeg/makepng.c

Method set_color(png_colorp color, png_bytep trans, unsigned int red,

```
....
243.      color->green = gamma_table[green];
```

Buffer Overflow Indexes\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=33
Status	New

The size of the buffer used by set_color in red, at line 238 of mobile-ffmpeg/makepng.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 1678 of mobile-ffmpeg/makepng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1678	242
Object	argv	red

Code Snippet

File Name mobile-ffmpeg/makepng.c

Method main(int argc, char **argv)

```
....
1678.  main(int argc, char **argv)
```

File Name mobile-ffmpeg/makepng.c

Method set_color(png_colorp color, png_bytep trans, unsigned int red,

```
....
242.     color->red = gamma_table[red];
```

Buffer Overflow Indexes\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=34
Status	New

The size of the buffer used by run_one_test in serverFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1161
Object	stdin	serverFinishedPermute

Code Snippet

File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c
Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1161.
      server_finished_permutation_names[serverFinishedPermute]);
```

Buffer Overflow Indexes\Path 35:

Severity High
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=35
Status New

The size of the buffer used by run_one_test in serverFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1108
Object	stdin	serverFinishedPermute

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c
Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1108.                 permutations2[serverFinishedPermute];
```

Buffer Overflow Indexes\Path 36:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=36
Status	New

The size of the buffer used by run_one_test in serverFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1112
Object	stdin	serverFinishedPermute

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c
Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1112.                   permutations3[serverFinishedPermute];
```

Buffer Overflow Indexes\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=37
Status	New

The size of the buffer used by run_one_test in serverFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1128
Object	stdin	serverFinishedPermute

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1128.                   permutations2[serverFinishedPermute];
```

Buffer Overflow Indexes\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=38
Status	New

The size of the buffer used by run_one_test in serverHelloPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1159
Object	stdin	serverHelloPermute

Code Snippet

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1159.               fprintf(stdout, "SHello(%s), ",
server_hello_permutation_names[serverHelloPermute]);
```

Buffer Overflow Indexes\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=39

Status	New

The size of the buffer used by run_one_test in serverHelloPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1100
Object	stdin	serverHelloPermute

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c
Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1100.                   permutations5[serverHelloPermute];
```

Buffer Overflow Indexes\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=40
Status	New

The size of the buffer used by run_one_test in serverHelloPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1120
Object	stdin	serverHelloPermute

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1120.                   permutations3[serverHelloPermute];
```

Buffer Overflow Indexes\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=41
Status	New

The size of the buffer used by run_one_test in clientFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1163
Object	stdin	clientFinishedPermute

Code Snippet

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1163.
      client_finished_permutation_names[clientFinishedPermute]);
```

Buffer Overflow Indexes\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=42

Status	New

The size of the buffer used by run_one_test in clientFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1104
Object	stdin	clientFinishedPermute

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c
Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1104.                permutations5[clientFinishedPermute];
```

Buffer Overflow Indexes\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=43
Status	New

The size of the buffer used by run_one_test in clientFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1116
Object	stdin	clientFinishedPermute

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1116.                   permutations2[clientFinishedPermute];
```

Buffer Overflow Indexes\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=44
Status	New

The size of the buffer used by run_one_test in clientFinishedPermute, at line 1056 of mobile-ffmpeg/dtls-stress.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that run_tests_from_id_list passes to stdin, at line 1255 of mobile-ffmpeg/dtls-stress.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1124
Object	stdin	clientFinishedPermute

Code Snippet

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

File Name mobile-ffmpeg/dtls-stress.c

Method static int run_one_test(int dropMode, int serverFinishedPermute,

```
....
1124.                   permutations3[clientFinishedPermute];
```

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=1060095&projectid=60085&pathid=45
Status	New

The size parameter BinaryExpr in line 636 in file mobile-ffmpeg/ath.c is influenced by the user input argv in line 775 in file mobile-ffmpeg/ath.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	693
Object	argv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/ath.c

Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c

Method int experiment (generator_t* const g,

```
....
693.                      sizeof(quant_errors[1]) -
sizeof(quant_errors[1][0]) );
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=46
Status	New

The size parameter BinaryExpr in line 636 in file mobile-ffmpeg/ath.c is influenced by the user input argv in line 775 in file mobile-ffmpeg/ath.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	775	665

Object	argv	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int main (int argc, char** argv)

```
....
775.  int main ( int argc, char** argv )
```

File Name mobile-ffmpeg/ath.c
Method int experiment (generator_t* const g,

```
....
665.                       sizeof(quant_errors[0]) -
sizeof(quant_errors[0][0]) );
```

Buffer Overflow boundedcpy\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=47
Status	New

The size parameter BinaryExpr in line 192 in file mobile-ffmpeg/getopt.c is influenced by the user input argc in line 1203 in file mobile-ffmpeg/getopt.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	222
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
222.                '\0', top + 1 - d->__nonoption_flags_max_len);
```

Buffer Overflow boundedcpy\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=48
Status	New

The size parameter BinaryExpr in line 192 in file mobile-ffmpeg/getopt.c is influenced by the user input argv in line 1203 in file mobile-ffmpeg/getopt.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	222
Object	argv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
222.                '\0', top + 1 - d->__nonoption_flags_max_len);
```

Buffer Overflow boundedcpy\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=49
Status	New

The size parameter BinaryExpr in line 192 in file mobile-ffmpeg/getopt.c is influenced by the user input getenv in line 276 in file mobile-ffmpeg/getopt.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	222
Object	getenv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
222.                '\0', top + 1 - d->__nonoption_flags_max_len);
```

Buffer Overflow boundedcpy\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=50
Status	New

The size parameter BinaryExpr in line 276 in file mobile-ffmpeg/getopt.c is influenced by the user input argc in line 1203 in file mobile-ffmpeg/getopt.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	330
Object	argc	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c

Method _getopt_initialize (

```
....
330.                    '\0', d->__nonoption_flags_max_len - len);
```

Buffer Overflow boundedcpy\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=51
Status	New

The size parameter rowbytes in line 390 in file mobile-ffmpeg/makepng.c is influenced by the user input argv in line 1678 in file mobile-ffmpeg/makepng.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1678	656
Object	argv	rowbytes

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1678.  main(int argc, char **argv)
```

File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
656.        memset(row, 0, rowbytes);
```

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=1060095&projectid=60085&pathid=255
Status	New

The size of the buffer used by new_extension in newname, at line 54 of mobile-ffmpeg/frontend.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 704 of mobile-ffmpeg/frontend.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c

Line	704	89
Object	argv	newname

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method int main(int argc, char **argv)

```
....
704.  int main(int argc, char **argv)
```

File Name mobile-ffmpeg/frontend.c
Method static void new_extension(char *filename, char *extname, char *newname)

```
....
89.           strcat(newname, extname);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=256
Status	New

The size of the buffer used by gl_locale_name_canonicalize in name, at line 1171 of mobile-ffmpeg/localename.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gl_locale_name_canonicalize passes to name, at line 1171 of mobile-ffmpeg/localename.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	1171	1400
Object	name	name

Code Snippet
File Name mobile-ffmpeg/localename.c
Method gl_locale_name_canonicalize (char *name)

```
....
1171.  gl_locale_name_canonicalize (char *name)
....
1400.             strcpy (name, legacy_table[i1].unixy);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=257

Status	New

The size of the buffer used by get_lcid in locale_name, at line 2602 of mobile-ffmpeg/localename.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_lcid passes to locale_name, at line 2602 of mobile-ffmpeg/localename.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	2602	2623
Object	locale_name	locale_name

Code Snippet
File Name mobile-ffmpeg/localename.c
Method get_lcid (const char *locale_name)

```
....
2602.  get_lcid (const char *locale_name)
....
2623.        strcpy (last_locale, locale_name);
```

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=1060095&projectid=60085&pathid=252
Status	New

The size of the buffer used by tune_divexact_1 in Address, at line 2563 of mobile-ffmpeg/tuneup.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tune_divexact_1 passes to "DIVEXACT_1_THRESHOLD", at line 2563 of mobile-ffmpeg/tuneup.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/tuneup.c	mobile-ffmpeg/tuneup.c
Line	2579	2598
Object	"DIVEXACT_1_THRESHOLD"	Address

Code Snippet
File Name mobile-ffmpeg/tuneup.c
Method tune_divexact_1 (void)

```
....
2579.    param.name = "DIVEXACT_1_THRESHOLD";
....
2598.        one (&thresh[low], &param);
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=253
Status	New

The size of the buffer used by tune_divexact_1 in Address, at line 2563 of mobile-ffmpeg/tuneup.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tune_div_qr_1 passes to "DIV_QR_1_UNNORM_THRESHOLD", at line 2251 of mobile-ffmpeg/tuneup.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/tuneup.c	mobile-ffmpeg/tuneup.c
Line	2280	2598
Object	"DIV_QR_1_UNNORM_THRESHOLD"	Address

Code Snippet
File Name mobile-ffmpeg/tuneup.c
Method tune_div_qr_1 (void)

```
....
2280.      param.name = "DIV_QR_1_UNNORM_THRESHOLD";
```

File Name mobile-ffmpeg/tuneup.c
Method tune_divexact_1 (void)

```
....
2598.        one (&thresh[low], &param);
```

String Termination Error

Query Path:
CPP\Cx\CPP Buffer Overflow\String Termination Error 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

String Termination Error\Path 1:

Severity	High
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=396
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	167	565
Object	Address	strlen

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int sel (void)

```
....
167.          ret = read (0, &c, 1);
```

File Name mobile-ffmpeg/abx.c
Method void Message (const char* s, size_t index, long freq, size_t start, size_t stop)

```
....
565.                36 - (int)strlen(s), 36 - (int)strlen(s), "",
```

String Termination Error\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=397
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	167	565
Object	Address	strlen

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int sel (void)

```
....
167.          ret = read (0, &c, 1);
```

File Name mobile-ffmpeg/abx.c
Method void Message (const char* s, size_t index, long freq, size_t start, size_t stop)

```
....
565.                36 - (int)strlen(s), 36 - (int)strlen(s), "",
```

Format String Attack

Query Path:
CPP\Cx\CPP Buffer Overflow\Format String Attack 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
Format String Attack\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=254
Status	New

Method select_input_res_auto at line 163 of mobile-ffmpeg/cli.c receives the "%dx%d%*s" value from user input. This value is then used to construct a "format string" "%dx%d%*s", which is provided as an argument to a string formatting function in select_input_res_auto method of mobile-ffmpeg/cli.c at line 163.

	Source	Destination
File	mobile-ffmpeg/cli.c	mobile-ffmpeg/cli.c
Line	175	175
Object	"%dx%d%*s"	"%dx%d%*s"

Code Snippet
File Name mobile-ffmpeg/cli.c
Method static int select_input_res_auto(const char *file_name, int32_t *out_width, int32_t *out_height)

```
....
175.      success = (sscanf((char*)sub_str, "%dx%d%*s", out_width,
out_height) == 2);
```

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=1060095&projectid=60085&pathid=562
Status	New

The dangerous function, alloca, was found in use at line 643 in mobile-ffmpeg/res0.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	662	662
Object	alloca	alloca

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static int _01inverse(vorbis_block *vb,vorbis_look_residue *vl,

```
....
662.      int ***partword=alloca(ch*sizeof(*partword));
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=563
Status	New

The dangerous function, memcpy, was found in use at line 949 in mobile-ffmpeg/colorquant2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/colorquant2.c	mobile-ffmpeg/colorquant2.c
Line	1054	1054
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/colorquant2.c
Method pixQuantizeWithColormap(PIX *pixs,

```
....
1054.             memcpy(buf1r, buf2r, 4 * w);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=564
Status	New

The dangerous function, memcpy, was found in use at line 949 in mobile-ffmpeg/colorquant2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/colorquant2.c	mobile-ffmpeg/colorquant2.c
Line	1055	1055
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/colorquant2.c
Method pixQuantizeWithColormap(PIX *pixs,

```
....
1055.               memcpy(buf1g, buf2g, 4 * w);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=565
Status	New

The dangerous function, memcpy, was found in use at line 949 in mobile-ffmpeg/colorquant2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/colorquant2.c	mobile-ffmpeg/colorquant2.c
Line	1056	1056
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/colorquant2.c
Method pixQuantizeWithColormap(PIX *pixs,

```
....
1056.               memcpy(buf1b, buf2b, 4 * w);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=566
Status	New

The dangerous function, memcpy, was found in use at line 136 in mobile-ffmpeg/DecUT_DecExt.cpp file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	159	159
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::DecoderBs (const char* sFileName) {

```
....
159.    memcpy (pBuf + iFileSize, &uiStartCode[0], 4);
//confirmed_safe_unsafe_usage
```

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=567
Status New

The dangerous function, memcpy, was found in use at line 228 in mobile-ffmpeg/DecUT_ParseSyntax.cpp file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	264	264
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method bool DecoderParseSyntaxTest::DecodeBs (const char* sFileName, EDecCase eDecCase) {

```
....
264.    memcpy (pBuf + iFileSize, &uiStartCode[0], 4);
//confirmed_safe_unsafe_usage
```

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=568
Status New

The dangerous function, memcpy, was found in use at line 295 in mobile-ffmpeg/DecUT_ParseSyntax.cpp file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	332	332
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method bool DecoderParseSyntaxTest::ParseBs (const char* sFileName, EDecCase eDecCase) {

```
....
332.    memcpy (pBuf + iFileSize, &uiStartCode[0], 4);
//confirmed_safe_unsafe_usage
```

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=569
Status New

The dangerous function, memcpy, was found in use at line 158 in mobile-ffmpeg/doprnt.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/doprnt.c	mobile-ffmpeg/doprnt.c
Line	190	190
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/doprnt.c
Method __gmp_doprnt (const struct doprnt_funs_t *funs, void *data,

```
....
190.    memcpy (fmt, orig_fmt, orig_fmt_size);
```

Dangerous Functions\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=570
Status New

The dangerous function, memcpy, was found in use at line 431 in mobile-ffmpeg/dtls-stress.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	446	446
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static void filter_run_next(gnutls_transport_ptr_t fd,

```
....
446.                    memcpy(rbuffer, buffer, len);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=571
Status	New

The dangerous function, memcpy, was found in use at line 431 in mobile-ffmpeg/dtls-stress.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	451	451
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static void filter_run_next(gnutls_transport_ptr_t fd,

```
....
451.                        memcpy(rbuffer, buffer, len);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=572
Status	New

The dangerous function, memcpy, was found in use at line 562 in mobile-ffmpeg/dtls-stress.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c

Line	573	573
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static void filter_permute_state_run(filter_permute_state_t * state,

```
....
573.        memcpy(data, buffer, len);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=573
Status	New

The dangerous function, memcpy, was found in use at line 826 in mobile-ffmpeg/dtls-stress.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	832	832
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static gnutls_datum_t db_fetch(void *dbf, gnutls_datum_t key)

```
....
832.        memcpy(t.data, saved_data.data, saved_data.size);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=574
Status	New

The dangerous function, memcpy, was found in use at line 843 in mobile-ffmpeg/dtls-stress.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	848	848
Object	memcpy	memcpy

Code Snippet	
File Name	mobile-ffmpeg/dtls-stress.c
Method	static int db_store(void *dbf, gnutls_datum_t key, gnutls_datum_t data)

```
....
848.        memcpy(saved_data.data, data.data, data.size);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=575
Status	New

The dangerous function, memcpy, was found in use at line 72 in mobile-ffmpeg/dwt.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/dwt.c	mobile-ffmpeg/dwt.c
Line	101	101
Object	memcpy	memcpy

Code Snippet	
File Name	mobile-ffmpeg/dwt.c
Method	static void dyadic_analyze_53_uint8_input(int levels, int width, int height,

```
....
101.        memcpy(buffer, &c[i * pitch_c], nw * sizeof(tran_low_t));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=576
Status	New

The dangerous function, memcpy, was found in use at line 1914 in mobile-ffmpeg/fpix2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/fpix2.c	mobile-ffmpeg/fpix2.c
Line	1940	1940
Object	memcpy	memcpy

Code Snippet	
File Name	mobile-ffmpeg/fpix2.c

Method	fpixFlipLR(FPIX *fpixd,

```
....
1940.          memcpy(buffer, line, bpl);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=577
Status	New

The dangerous function, memcpy, was found in use at line 1975 in mobile-ffmpeg/fpix2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/fpix2.c	mobile-ffmpeg/fpix2.c
Line	2002	2002
Object	memcpy	memcpy

Code Snippet	
File Name	mobile-ffmpeg/fpix2.c
Method	fpixFlipTB(FPIX *fpixd,

```
....
2002.          memcpy(buffer, linet, bpl);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=578
Status	New

The dangerous function, memcpy, was found in use at line 1975 in mobile-ffmpeg/fpix2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/fpix2.c	mobile-ffmpeg/fpix2.c
Line	2003	2003
Object	memcpy	memcpy

Code Snippet	
File Name	mobile-ffmpeg/fpix2.c
Method	fpixFlipTB(FPIX *fpixd,

```
....
2003.          memcpy(linet, lineb, bpl);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=579
Status	New

The dangerous function, memcpy, was found in use at line 1975 in mobile-ffmpeg/fpix2.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/fpix2.c	mobile-ffmpeg/fpix2.c
Line	2004	2004
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/fpix2.c
Method fpixFlipTB(FPIX *fpixd,

```
....
2004.          memcpy(lineb, buffer, bpl);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=580
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1843	1843
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1843.
memcpy(ogg_sync_buffer(&oy,og[i].header_len),og[i].header,
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=581
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1846	1846
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1846.
memcpy(ogg_sync_buffer(&oy,og[i].body_len),og[i].body,og[i].body_len);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=582
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1892	1892
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1892.
memcpy(ogg_sync_buffer(&oy,og[i].header_len),og[i].header,
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=583
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1895	1895
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1895.
memcpy(ogg_sync_buffer(&oy,og[i].body_len),og[i].body,og[i].body_len);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=584
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1945	1945
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1945.        memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header,
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=585
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1951	1951
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1951.
memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header+3,
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=586
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1957	1957
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1957.
memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header+23,
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=587
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1964	1964
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1964.
memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header+28,
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=588
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1969	1969
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1969.
memcpy(ogg_sync_buffer(&oy,og[1].body_len),og[1].body,1000);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=589
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1973	1973
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1973.        memcpy(ogg_sync_buffer(&oy,og[1].body_len),og[1].body+1000,
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=590
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1987	1987
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1987.        memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header,
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=591
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1991	1991
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1991.        memcpy(ogg_sync_buffer(&oy,og[1].body_len),og[1].body,
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=592
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	1995	1995
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
1995.        memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header,
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=593
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2001	2001
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2001.
memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header+20,
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=594
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2004	2004
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2004.        memcpy(ogg_sync_buffer(&oy,og[1].body_len),og[1].body,
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=595
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2019	2019
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2019.        memcpy(ogg_sync_buffer(&oy,og[1].body_len),og[1].body,
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=596
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2023	2023
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2023.        memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header,
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=597
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2027	2027
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2027.        memcpy(ogg_sync_buffer(&oy,og[1].body_len),og[1].body,
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=598
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2031	2031
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2031.        memcpy(ogg_sync_buffer(&oy,og[2].header_len),og[2].header,
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=599
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2038	2038
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2038.
memcpy(ogg_sync_buffer(&oy,og[2].header_len),og[2].header+20,
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=600
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2041	2041
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2041.        memcpy(ogg_sync_buffer(&oy,og[2].body_len),og[2].body,
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=601
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2056	2056
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2056.        memcpy(ogg_sync_buffer(&oy,og[1].header_len),og[1].header,
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=602
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2060	2060
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2060.        memcpy(ogg_sync_buffer(&oy,og[1].body_len),og[1].body,
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=603
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2064	2064
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2064.        memcpy(ogg_sync_buffer(&oy,og[2].header_len),og[2].header,
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=604
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2068	2068
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2068.        memcpy(ogg_sync_buffer(&oy,og[2].header_len),og[2].header,
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=605
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2074	2074
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2074.        memcpy(ogg_sync_buffer(&oy,og[2].body_len),og[2].body,
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=606
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2078	2078
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2078.         memcpy(ogg_sync_buffer(&oy,og[3].header_len),og[3].header,
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=607
Status	New

The dangerous function, memcpy, was found in use at line 1661 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	2082	2082
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int main(void){

```
....
2082.         memcpy(ogg_sync_buffer(&oy,og[3].body_len),og[3].body,
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=608
Status	New

The dangerous function, memcpy, was found in use at line 276 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	314	314
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method int ogg_stream_iovecin(ogg_stream_state *os, ogg_iovec_t *iov, int count,

```
....
314.      memcpy(os->body_data+os->body_fill, iov[i].iov_base,
iov[i].iov_len);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=609
Status	New

The dangerous function, memcpy, was found in use at line 349 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	404	404
Object	memcpy	memcpy

Code Snippet

File Name mobile-ffmpeg/framing.c

Method static int ogg_stream_flush_i(ogg_stream_state *os,ogg_page *og, int force, int nfill){

```
....
404.    memcpy(os->header,"OggS",4);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=610
Status	New

The dangerous function, memcpy, was found in use at line 636 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	668	668
Object	memcpy	memcpy

Code Snippet

File Name mobile-ffmpeg/framing.c

Method long ogg_sync_pageseek(ogg_sync_state *oy,ogg_page *og){

```
....
668.        memcpy(chksum,page+22,4);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=611
Status	New

The dangerous function, memcpy, was found in use at line 636 in mobile-ffmpeg/framing.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	683	683
Object	memcpy	memcpy

Code Snippet
File Name mobile-ffmpeg/framing.c
Method long ogg_sync_pageseek(ogg_sync_state *oy,ogg_page *og){

```
....
683.        memcpy(page+22,chksum,4);
```

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=1060095&projectid=60085&pathid=258
Status	New

The size of the buffer used by oc_state_init in _info, at line 617 of mobile-ffmpeg/state.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oc_state_init passes to _info, at line 617 of mobile-ffmpeg/state.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	646	646

Object	_info	_info

Code Snippet
File Name mobile-ffmpeg/state.c
Method int oc_state_init(oc_theora_state *_state,const th_info *_info,int _nrefs){

```
....
646.    memcpy(&_state->info,_info,sizeof(*_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=259
Status	New

The size of the buffer used by DecoderInterfaceTest::Init in SBufferInfo, at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::Init passes to SBufferInfo, at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	86	86
Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::Init() {

```
....
86.    memset (&m_sBufferInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=260
Status	New

The size of the buffer used by DecoderInterfaceTest::Init in SParserBsInfo, at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::Init passes to SParserBsInfo, at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	87	87

Object	SParserBsInfo	SParserBsInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::Init() {

```
....
87.    memset (&m_sParserBsInfo, 0, sizeof (SParserBsInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=261
Status	New

The size of the buffer used by DecoderInterfaceTest::Init in SDecodingParam, at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::Init passes to SDecodingParam, at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	88	88
Object	SDecodingParam	SDecodingParam

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::Init() {

```
....
88.    memset (&m_sDecParam, 0, sizeof (SDecodingParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=262
Status	New

The size of the buffer used by DecoderInterfaceTest::ValidInit in SBufferInfo, at line 105 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::ValidInit passes to SBufferInfo, at line 105 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	106	106

Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::ValidInit() {

```
....
106.    memset (&m_sBufferInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=263
Status	New

The size of the buffer used by DecoderInterfaceTest::ValidInit in SDecodingParam, at line 105 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::ValidInit passes to SDecodingParam, at line 105 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	107	107
Object	SDecodingParam	SDecodingParam

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::ValidInit() {

```
....
107.    memset (&m_sDecParam, 0, sizeof (SDecodingParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=264
Status	New

The size of the buffer used by DecoderInterfaceTest::Uninit in SDecodingParam, at line 124 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::Uninit passes to SDecodingParam, at line 124 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	129	129

Object	SDecodingParam	SDecodingParam

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::Uninit() {

```
....
129.    memset (&m_sDecParam, 0, sizeof (SDecodingParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=265
Status	New

The size of the buffer used by DecoderInterfaceTest::Uninit in SParserBsInfo, at line 124 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::Uninit passes to SParserBsInfo, at line 124 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	130	130
Object	SParserBsInfo	SParserBsInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::Uninit() {

```
....
130.    memset (&m_sParserBsInfo, 0, sizeof (SParserBsInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=266
Status	New

The size of the buffer used by DecoderInterfaceTest::Uninit in SBufferInfo, at line 124 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::Uninit passes to SBufferInfo, at line 124 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	131	131

Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::Uninit() {

```
....
131.    memset (&m_sBufferInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=267
Status	New

The size of the buffer used by DecoderInterfaceTest::TestParseOnlyAPI in SBufferInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::TestParseOnlyAPI passes to SBufferInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	274	274
Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
274.      memset (&m_sBufferInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=268
Status	New

The size of the buffer used by DecoderInterfaceTest::TestParseOnlyAPI in SParserBsInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::TestParseOnlyAPI passes to SParserBsInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	275	275

Object	SParserBsInfo	SParserBsInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
275.      memset (&m_sParserBsInfo, 0, sizeof (SParserBsInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=269
Status New

The size of the buffer used by DecoderInterfaceTest::TestParseOnlyAPI in SDecodingParam, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::TestParseOnlyAPI passes to SDecodingParam, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	276	276
Object	SDecodingParam	SDecodingParam

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
276.      memset (&m_sDecParam, 0, sizeof (SDecodingParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=270
Status New

The size of the buffer used by DecoderInterfaceTest::TestParseOnlyAPI in SBufferInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::TestParseOnlyAPI passes to SBufferInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	307	307

Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
307.      memset (&m_sBufferInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=271
Status New

The size of the buffer used by DecoderInterfaceTest::TestParseOnlyAPI in SParserBsInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::TestParseOnlyAPI passes to SParserBsInfo, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	308	308
Object	SParserBsInfo	SParserBsInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
308.      memset (&m_sParserBsInfo, 0, sizeof (SParserBsInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=272
Status New

The size of the buffer used by DecoderInterfaceTest::TestParseOnlyAPI in SDecodingParam, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderInterfaceTest::TestParseOnlyAPI passes to SDecodingParam, at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	309	309

Object	SDecodingParam	SDecodingParam

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
309.      memset (&m_sDecParam, 0, sizeof (SDecodingParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=273
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SBufferInfo, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SBufferInfo, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	173	173
Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
173.    memset (&m_sBufferInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=274
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SDecodingParam, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SDecodingParam, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	174	174

Object	SDecodingParam	SDecodingParam

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
174.    memset (&m_sDecParam, 0, sizeof (SDecodingParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=275
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SParserBsInfo, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SParserBsInfo, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	175	175
Object	SParserBsInfo	SParserBsInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
175.    memset (&m_sParserBsInfo, 0, sizeof (SParserBsInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=276
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SWelsDecoderSpsPpsCTX, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SWelsDecoderSpsPpsCTX, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	176	176

Object	SWelsDecoderSpsPpsCTX	SWelsDecoderSpsPpsCTX

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
176.    memset (&m_sDecoderSpsPpsCTX, 0, sizeof
(SWelsDecoderSpsPpsCTX));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=277
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SWelsLastDecPicInfo, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SWelsLastDecPicInfo, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	177	177
Object	SWelsLastDecPicInfo	SWelsLastDecPicInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
177.    memset (&m_sLastDecPicInfo, 0, sizeof (SWelsLastDecPicInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=278
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SDecoderStatistics, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SDecoderStatistics, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	178	178

Object	SDecoderStatistics	SDecoderStatistics

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
178.    memset (&m_sDecoderStatistics, 0, sizeof (SDecoderStatistics));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=279
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SVlcTable, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SVlcTable, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	179	179
Object	SVlcTable	SVlcTable

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
179.    memset (&m_sVlcTable, 0, sizeof (SVlcTable));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=280
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Init in SWelsDecoderContext, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Init passes to SWelsDecoderContext, at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	197	197

Object	SWelsDecoderContext	SWelsDecoderContext

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
197.    memset (m_pCtx, 0, sizeof (SWelsDecoderContext));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=281
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Uninit in SDecodingParam, at line 214 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Uninit passes to SDecodingParam, at line 214 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	222	222
Object	SDecodingParam	SDecodingParam

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method void DecoderParseSyntaxTest::Uninit() {

```
....
222.    memset (&m_sDecParam, 0, sizeof (SDecodingParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=282
Status	New

The size of the buffer used by DecoderParseSyntaxTest::Uninit in SBufferInfo, at line 214 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::Uninit passes to SBufferInfo, at line 214 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	223	223

Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method void DecoderParseSyntaxTest::Uninit() {

```
....
223.    memset (&m_sBufferInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=283
Status	New

The size of the buffer used by DecoderParseSyntaxTest::ParseBs in SParserBsInfo, at line 295 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecoderParseSyntaxTest::ParseBs passes to SParserBsInfo, at line 295 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	347	347
Object	SParserBsInfo	SParserBsInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method bool DecoderParseSyntaxTest::ParseBs (const char* sFileName, EDecCase eDecCase) {

```
....
347.      memset (&m_sParserBsInfo, 0, sizeof (SParserBsInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=284
Status	New

The size of the buffer used by DecodeFrame in SBufferInfo, at line 21 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DecodeFrame passes to SBufferInfo, at line 21 of mobile-ffmpeg/DecUT_ParseSyntax.cpp, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	44	44

Object	SBufferInfo	SBufferInfo

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method DECODING_STATE DecodeFrame (const unsigned char* kpSrc,

```
....
44.    memset (pDstInfo, 0, sizeof (SBufferInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=285
Status	New

The size of the buffer used by ReadJPEG in dinfo, at line 258 of mobile-ffmpeg/jpegdec.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ReadJPEG passes to dinfo, at line 258 of mobile-ffmpeg/jpegdec.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/jpegdec.c	mobile-ffmpeg/jpegdec.c
Line	277	277
Object	dinfo	dinfo

Code Snippet
File Name mobile-ffmpeg/jpegdec.c
Method int ReadJPEG(const uint8_t* const data, size_t data_size,

```
....
277.    memset((j_decompress_ptr)&dinfo, 0, sizeof(dinfo));   // for
setjmp sanity
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=286
Status	New

The size of the buffer used by oc_sb_create_plane_mapping in _sb_maps, at line 55 of mobile-ffmpeg/state.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oc_sb_create_plane_mapping passes to _sb_maps, at line 55 of mobile-ffmpeg/state.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	95	95

Object	_sb_maps	_sb_maps

Code Snippet
File Name mobile-ffmpeg/state.c
Method static void oc_sb_create_plane_mapping(oc_sb_map _sb_maps[],

```
....
95.         memset(_sb_maps[sbi][0],0xFF,sizeof(_sb_maps[sbi]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=287
Status New

The size of the buffer used by oc_sb_create_plane_mapping in sbi, at line 55 of mobile-ffmpeg/state.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oc_sb_create_plane_mapping passes to sbi, at line 55 of mobile-ffmpeg/state.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	95	95
Object	sbi	sbi

Code Snippet
File Name mobile-ffmpeg/state.c
Method static void oc_sb_create_plane_mapping(oc_sb_map _sb_maps[],

```
....
95.         memset(_sb_maps[sbi][0],0xFF,sizeof(_sb_maps[sbi]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=288
Status New

The size of the buffer used by oc_mb_create_mapping in _mb_maps, at line 224 of mobile-ffmpeg/state.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oc_mb_create_mapping passes to _mb_maps, at line 224 of mobile-ffmpeg/state.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	246	246

Object	_mb_maps	_mb_maps

Code Snippet
File Name mobile-ffmpeg/state.c
Method static void oc_mb_create_mapping(oc_mb_map _mb_maps[],

```
....
246.            memset(_mb_maps[mbi],0xFF,sizeof(_mb_maps[mbi]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=289
Status	New

The size of the buffer used by oc_mb_create_mapping in mbi, at line 224 of mobile-ffmpeg/state.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oc_mb_create_mapping passes to mbi, at line 224 of mobile-ffmpeg/state.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	246	246
Object	mbi	mbi

Code Snippet
File Name mobile-ffmpeg/state.c
Method static void oc_mb_create_mapping(oc_mb_map _mb_maps[],

```
....
246.            memset(_mb_maps[mbi],0xFF,sizeof(_mb_maps[mbi]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=290
Status	New

The size of the buffer used by streebog512_init in ->, at line 1254 of mobile-ffmpeg/streebog.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streebog512_init passes to ->, at line 1254 of mobile-ffmpeg/streebog.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/streebog.c	mobile-ffmpeg/streebog.c
Line	1256	1256
Object	->	->

Code Snippet
File Name mobile-ffmpeg/streebog.c
Method streebog512_init(struct streebog512_ctx *ctx)

```
....
1256.    memset(ctx->state, 0, sizeof(ctx->state));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=291
Status	New

The size of the buffer used by streebog512_init in ->, at line 1254 of mobile-ffmpeg/streebog.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streebog512_init passes to ->, at line 1254 of mobile-ffmpeg/streebog.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/streebog.c	mobile-ffmpeg/streebog.c
Line	1257	1257
Object	->	->

Code Snippet
File Name mobile-ffmpeg/streebog.c
Method streebog512_init(struct streebog512_ctx *ctx)

```
....
1257.    memset(ctx->count, 0, sizeof(ctx->count));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=292
Status	New

The size of the buffer used by streebog512_init in ->, at line 1254 of mobile-ffmpeg/streebog.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streebog512_init passes to ->, at line 1254 of mobile-ffmpeg/streebog.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/streebog.c	mobile-ffmpeg/streebog.c
Line	1258	1258
Object	->	->

Code Snippet
File Name mobile-ffmpeg/streebog.c

Method	streebog512_init(struct streebog512_ctx *ctx)

```
....
1258.    memset(ctx->sigma, 0, sizeof(ctx->sigma));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=293
Status	New

The size of the buffer used by streebog256_init in ->, at line 1314 of mobile-ffmpeg/streebog.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streebog256_init passes to ->, at line 1314 of mobile-ffmpeg/streebog.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/streebog.c	mobile-ffmpeg/streebog.c
Line	1316	1316
Object	->	->

Code Snippet	
File Name	mobile-ffmpeg/streebog.c
Method	streebog256_init(struct streebog256_ctx *ctx)

```
....
1316.    memset(ctx->state, 1, sizeof(ctx->state));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=294
Status	New

The size of the buffer used by streebog256_init in ->, at line 1314 of mobile-ffmpeg/streebog.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streebog256_init passes to ->, at line 1314 of mobile-ffmpeg/streebog.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/streebog.c	mobile-ffmpeg/streebog.c
Line	1317	1317
Object	->	->

Code Snippet	
File Name	mobile-ffmpeg/streebog.c
Method	streebog256_init(struct streebog256_ctx *ctx)

```
....
1317.    memset(ctx->count, 0, sizeof(ctx->count));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=295
Status	New

The size of the buffer used by streebog256_init in ->, at line 1314 of mobile-ffmpeg/streebog.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streebog256_init passes to ->, at line 1314 of mobile-ffmpeg/streebog.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/streebog.c	mobile-ffmpeg/streebog.c
Line	1318	1318
Object	->	->

Code Snippet
File Name mobile-ffmpeg/streebog.c
Method streebog256_init(struct streebog256_ctx *ctx)

```
....
1318.    memset(ctx->sigma, 0, sizeof(ctx->sigma));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=296
Status	New

The size of the buffer used by wavlike_read_fmt_chunk in WAV_FMT, at line 124 of mobile-ffmpeg/wavlike.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that wavlike_read_fmt_chunk passes to WAV_FMT, at line 124 of mobile-ffmpeg/wavlike.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/wavlike.c	mobile-ffmpeg/wavlike.c
Line	133	133
Object	WAV_FMT	WAV_FMT

Code Snippet
File Name mobile-ffmpeg/wavlike.c
Method wavlike_read_fmt_chunk (SF_PRIVATE *psf, int fmtsize)

```
....
133.        memset (wav_fmt, 0, sizeof (WAV_FMT)) ;
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=297
Status	New

The size of the buffer used by wavex_guid_equal in EXT_SUBFORMAT, at line 117 of mobile-ffmpeg/wavlike.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that wavex_guid_equal passes to EXT_SUBFORMAT, at line 117 of mobile-ffmpeg/wavlike.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/wavlike.c	mobile-ffmpeg/wavlike.c
Line	118	118
Object	EXT_SUBFORMAT	EXT_SUBFORMAT

Code Snippet
File Name mobile-ffmpeg/wavlike.c
Method wavex_guid_equal (const EXT_SUBFORMAT * first, const EXT_SUBFORMAT * second)

```
....
118.  {     return !memcmp (first, second, sizeof (EXT_SUBFORMAT)) ;
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=298
Status	New

The size of the buffer used by dyadic_analyze_53_uint8_input in nw, at line 72 of mobile-ffmpeg/dwt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dyadic_analyze_53_uint8_input passes to nw, at line 72 of mobile-ffmpeg/dwt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dwt.c	mobile-ffmpeg/dwt.c
Line	101	101
Object	nw	nw

Code Snippet
File Name mobile-ffmpeg/dwt.c
Method static void dyadic_analyze_53_uint8_input(int levels, int width, int height,

```
....
101.        memcpy(buffer, &c[i * pitch_c], nw * sizeof(tran_low_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=299
Status	New

The size of the buffer used by dyadic_analyze_53_uint8_input in tran_low_t, at line 72 of mobile-ffmpeg/dwt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dyadic_analyze_53_uint8_input passes to tran_low_t, at line 72 of mobile-ffmpeg/dwt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/dwt.c	mobile-ffmpeg/dwt.c
Line	101	101
Object	tran_low_t	tran_low_t

Code Snippet
File Name mobile-ffmpeg/dwt.c
Method static void dyadic_analyze_53_uint8_input(int levels, int width, int height,

```
....
101.        memcpy(buffer, &c[i * pitch_c], nw * sizeof(tran_low_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=300
Status	New

The size of the buffer used by yuv_io_extract_field in frame_in, at line 199 of mobile-ffmpeg/kvazaar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that yuv_io_extract_field passes to frame_in, at line 199 of mobile-ffmpeg/kvazaar.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	212	212
Object	frame_in	frame_in

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static int yuv_io_extract_field(const kvz_picture *frame_in, unsigned source_scan_type, unsigned field_parity, kvz_picture *field_out)

```
....
212.      memcpy(row_out, row_in, sizeof(kvz_pixel) * frame_in->width);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=301
Status	New

The size of the buffer used by yuv_io_extract_field in kvz_pixel, at line 199 of mobile-ffmpeg/kvazaar.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that yuv_io_extract_field passes to kvz_pixel, at line 199 of mobile-ffmpeg/kvazaar.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	212	212
Object	kvz_pixel	kvz_pixel

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static int yuv_io_extract_field(const kvz_picture *frame_in, unsigned source_scan_type, unsigned field_parity, kvz_picture *field_out)

```
....
212.      memcpy(row_out, row_in, sizeof(kvz_pixel) * frame_in->width);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=302
Status	New

The size of the buffer used by ransac in npoints, at line 372 of mobile-ffmpeg/ransac.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ransac passes to npoints, at line 372 of mobile-ffmpeg/ransac.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	503	503
Object	npoints	npoints

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
503.                sizeof(*current_motion.inlier_indices) * npoints);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=303
Status	New

The size of the buffer used by ransac in current_motion, at line 372 of mobile-ffmpeg/ransac.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ransac passes to current_motion, at line 372 of mobile-ffmpeg/ransac.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	503	503
Object	current_motion	current_motion

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
503.                sizeof(*current_motion.inlier_indices) * npoints);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=304
Status	New

The size of the buffer used by ransac in npoints, at line 372 of mobile-ffmpeg/ransac.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ransac passes to npoints, at line 372 of mobile-ffmpeg/ransac.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	532	532
Object	npoints	npoints

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
532.                sizeof(*motions[i].inlier_indices) * npoints);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=305
Status	New

The size of the buffer used by ransac in motions, at line 372 of mobile-ffmpeg/ransac.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ransac passes to motions, at line 372 of mobile-ffmpeg/ransac.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	532	532
Object	motions	motions

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
532.                sizeof(*motions[i].inlier_indices) * npoints);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=306
Status	New

The size of the buffer used by ransac in i, at line 372 of mobile-ffmpeg/ransac.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ransac passes to i, at line 372 of mobile-ffmpeg/ransac.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	532	532
Object	i	i

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
532.                sizeof(*motions[i].inlier_indices) * npoints);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=307
Status	New

The size of the buffer used by ransac_double_prec in npoints, at line 552 of mobile-ffmpeg/ransac.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ransac_double_prec passes to npoints, at line 552 of mobile-ffmpeg/ransac.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	684	684
Object	npoints	npoints

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac_double_prec(const double *matched_points, int npoints,

```
....
684.                sizeof(*current_motion.inlier_indices) * npoints);
```

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=1060095&projectid=60085&pathid=398
Status	New

The application performs an illegal operation in t2p_read_tiff_init, in mobile-ffmpeg/tiff2pdf.c. In line 1045, the program attempts to divide by xuint16, 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 xuint16 in t2p_read_tiff_init of mobile-ffmpeg/tiff2pdf.c, at line 1045.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1235	1235
Object	xuint16	xuint16

Code Snippet	
File Name	mobile-ffmpeg/tiff2pdf.c
Method	void t2p_read_tiff_init(T2P* t2p, TIFF* input){

```
....
1235.                           t2p->tiff_tiles[i].tiles_tilecount/=
xuint16;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=399
Status	New

The application performs an illegal operation in setup, in mobile-ffmpeg/abx.c. In line 525, the program attempts to divide by arg, 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 arg in setup of mobile-ffmpeg/abx.c, at line 525.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	549	549
Object	arg	arg

Code Snippet	
File Name	mobile-ffmpeg/abx.c
Method	void setup (int fdd, int samples, long freq)

```
....
549.      fprintf (stderr, "%5u Hz*%.3f sec\n", arg, (double)samples/arg
);
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=400
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMap, in mobile-ffmpeg/adaptmap.c. In line 852, the program attempts to divide by sx, 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 sx in pixGetBackgroundGrayMap of mobile-ffmpeg/adaptmap.c, at line 852.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	912	912

Object	sx	sx

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMap(PIX *pixs,

```
....
912.      wd = (w + sx - 1) / sx;
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=401
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMap, in mobile-ffmpeg/adaptmap.c. In line 852, the program attempts to divide by sy, 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 sy in pixGetBackgroundGrayMap of mobile-ffmpeg/adaptmap.c, at line 852.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	913	913
Object	sy	sy

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMap(PIX *pixs,

```
....
913.      hd = (h + sy - 1) / sy;
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=402
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMap, in mobile-ffmpeg/adaptmap.c. In line 852, the program attempts to divide by sx, 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 sx in pixGetBackgroundGrayMap of mobile-ffmpeg/adaptmap.c, at line 852.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c

Line	919	919
Object	sx	sx

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMap(PIX *pixs,

```
....
919.        nx = w / sx;
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=403
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMap, in mobile-ffmpeg/adaptmap.c. In line 852, the program attempts to divide by sy, 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 sy in pixGetBackgroundGrayMap of mobile-ffmpeg/adaptmap.c, at line 852.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	920	920
Object	sy	sy

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMap(PIX *pixs,

```
....
920.        ny = h / sy;
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=404
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMap, in mobile-ffmpeg/adaptmap.c. In line 852, the program attempts to divide by count, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input count in pixGetBackgroundGrayMap of mobile-ffmpeg/adaptmap.c, at line 852.

	Source	Destination

File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	944	944
Object	count	count

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMap(PIX *pixs,

```
....
944.                    val8 = sum / count;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=405
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMap, in mobile-ffmpeg/adaptmap.c. In line 852, the program attempts to divide by sx, 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 sx in pixGetBackgroundGrayMap of mobile-ffmpeg/adaptmap.c, at line 852.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	995	995
Object	sx	sx

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMap(PIX *pixs,

```
....
995.            scalex = 1. / (l_float32)sx;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=406
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMap, in mobile-ffmpeg/adaptmap.c. In line 852, the program attempts to divide by sy, 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 sy in pixGetBackgroundGrayMap of mobile-ffmpeg/adaptmap.c, at line 852.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	996	996
Object	sy	sy

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMap(PIX *pixs,

```
....
996.          scaley = 1. / (l_float32)sy;
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=407
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by sx, 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 sx in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1098	1098
Object	sx	sx

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1098.       wm = (w + sx - 1) / sx;
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=408
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by sy, 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 sy in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1099	1099
Object	sy	sy

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1099.       hm = (h + sy - 1) / sy;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=409
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by sx, 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 sx in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1108	1108
Object	sx	sx

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1108.       nx = w / sx;
```

Divide By Zero\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=410
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by sy, 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 sy in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1109	1109
Object	sy	sy

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1109.       ny = h / sy;
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=411
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by count, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input count in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1133	1133
Object	count	count

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1133.                   rval = rsum / count;
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=412
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by count, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input count in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1134	1134
Object	count	count

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1134.                    gval = gsum / count;
```

Divide By Zero\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=413
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by count, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input count in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1135	1135
Object	count	count

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1135.                    bval = bsum / count;
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=414
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by sx, 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 sx in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1186	1186
Object	sx	sx

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1186.          scalex = 1. / (l_float32)sx;
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=415
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMap, in mobile-ffmpeg/adaptmap.c. In line 1032, the program attempts to divide by sy, 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 sy in pixGetBackgroundRGBMap of mobile-ffmpeg/adaptmap.c, at line 1032.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1187	1187
Object	sy	sy

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMap(PIX *pixs,

```
....
1187.          scaley = 1. / (l_float32)sy;
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=416
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMapMorph, in mobile-ffmpeg/adaptmap.c. In line 1217, the program attempts to divide by reduction, 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 reduction in pixGetBackgroundGrayMapMorph of mobile-ffmpeg/adaptmap.c, at line 1217.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1253	1253
Object	reduction	reduction

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMapMorph(PIX *pixs,

```
....
1253.       scale = 1. / (l_float32)reduction;
```

Divide By Zero\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=417
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMapMorph, in mobile-ffmpeg/adaptmap.c. In line 1217, the program attempts to divide by reduction, 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 reduction in pixGetBackgroundGrayMapMorph of mobile-ffmpeg/adaptmap.c, at line 1217.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1273	1273
Object	reduction	reduction

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMapMorph(PIX *pixs,

```
....
1273.       nx = pixGetWidth(pixs) / reduction;
```

Divide By Zero\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=418
Status	New

The application performs an illegal operation in pixGetBackgroundGrayMapMorph, in mobile-ffmpeg/adaptmap.c. In line 1217, the program attempts to divide by reduction, 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 reduction in pixGetBackgroundGrayMapMorph of mobile-ffmpeg/adaptmap.c, at line 1217.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1274	1274
Object	reduction	reduction

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundGrayMapMorph(PIX *pixs,

```
....
1274.       ny = pixGetHeight(pixs) / reduction;
```

Divide By Zero\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=419
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMapMorph, in mobile-ffmpeg/adaptmap.c. In line 1308, the program attempts to divide by reduction, 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 reduction in pixGetBackgroundRGBMapMorph of mobile-ffmpeg/adaptmap.c, at line 1308.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1346	1346
Object	reduction	reduction

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMapMorph(PIX *pixs,

```
....
1346.       scale = 1. / (l_float32)reduction;
```

Divide By Zero\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=420
Status	New

The application performs an illegal operation in pixGetBackgroundRGBMapMorph, in mobile-ffmpeg/adaptmap.c. In line 1308, the program attempts to divide by reduction, 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 reduction in pixGetBackgroundRGBMapMorph of mobile-ffmpeg/adaptmap.c, at line 1308.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1392	1392
Object	reduction	reduction

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMapMorph(PIX *pixs,

```
....
1392.       nx = pixGetWidth(pixs) / reduction;
```

Divide By Zero\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=421
Status New

The application performs an illegal operation in pixGetBackgroundRGBMapMorph, in mobile-ffmpeg/adaptmap.c. In line 1308, the program attempts to divide by reduction, 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 reduction in pixGetBackgroundRGBMapMorph of mobile-ffmpeg/adaptmap.c, at line 1308.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	1393	1393
Object	reduction	reduction

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGetBackgroundRGBMapMorph(PIX *pixs,

```
....
1393.       ny = pixGetHeight(pixs) / reduction;
```

Divide By Zero\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=422
Status New

The application performs an illegal operation in pixGlobalNormNoSatRGB, in mobile-ffmpeg/adaptmap.c. In line 2292, the program attempts to divide by rval, 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 rval in pixGlobalNormNoSatRGB of mobile-ffmpeg/adaptmap.c, at line 2292.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	2329	2329
Object	rval	rval

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGlobalNormNoSatRGB(PIX *pixd,

```
....
2329.       rfract = rankrval / (l_float32)rval;
```

Divide By Zero\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=423
Status New

The application performs an illegal operation in pixGlobalNormNoSatRGB, in mobile-ffmpeg/adaptmap.c. In line 2292, the program attempts to divide by gval, 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 gval in pixGlobalNormNoSatRGB of mobile-ffmpeg/adaptmap.c, at line 2292.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	2330	2330
Object	gval	gval

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGlobalNormNoSatRGB(PIX *pixd,

```
....
2330.       gfract = rankgval / (l_float32)gval;
```

Divide By Zero\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=424
Status New

The application performs an illegal operation in pixGlobalNormNoSatRGB, in mobile-ffmpeg/adaptmap.c. In line 2292, the program attempts to divide by bval, 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 bval in pixGlobalNormNoSatRGB of mobile-ffmpeg/adaptmap.c, at line 2292.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	2331	2331
Object	bval	bval

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixGlobalNormNoSatRGB(PIX *pixd,

```
....
2331.      bfract = rankbval / (l_float32)bval;
```

Divide By Zero\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=425
Status	New

The application performs an illegal operation in pixBackgroundNormFlex, in mobile-ffmpeg/adaptmap.c. In line 2500, the program attempts to divide by sx, 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 sx in pixBackgroundNormFlex of mobile-ffmpeg/adaptmap.c, at line 2500.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	2526	2526
Object	sx	sx

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixBackgroundNormFlex(PIX *pixs,

```
....
2526.      scalex = 1. / (l_float32)sx;
```

Divide By Zero\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=426
Status	New

The application performs an illegal operation in pixBackgroundNormFlex, in mobile-ffmpeg/adaptmap.c. In line 2500, the program attempts to divide by sy, 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 sy in pixBackgroundNormFlex of mobile-ffmpeg/adaptmap.c, at line 2500.

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	2527	2527
Object	sy	sy

Code Snippet
File Name mobile-ffmpeg/adaptmap.c
Method pixBackgroundNormFlex(PIX *pixs,

```
....
2527.      scaley = 1. / (l_float32)sy;
```

Divide By Zero\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=427
Status	New

The application performs an illegal operation in pixMedianCutQuantMixed, in mobile-ffmpeg/colorquant2.c. In line 579, the program attempts to divide by BinaryExpr, 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 BinaryExpr in pixMedianCutQuantMixed of mobile-ffmpeg/colorquant2.c, at line 579.

	Source	Destination
File	mobile-ffmpeg/colorquant2.c	mobile-ffmpeg/colorquant2.c
Line	678	678
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/colorquant2.c
Method pixMedianCutQuantMixed(PIX *pixs,

```
....
678.          grayval = (255 * i) / (ngray - 1);
```

Divide By Zero\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=428
Status	New

The application performs an illegal operation in displayHSVColorRange, in mobile-ffmpeg/colorspace.c. In line 1378, the program attempts to divide by nsamp, 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 nsamp in displayHSVColorRange of mobile-ffmpeg/colorspace.c, at line 1378.

	Source	Destination
File	mobile-ffmpeg/colorspace.c	mobile-ffmpeg/colorspace.c
Line	1403	1403
Object	nsamp	nsamp

Code Snippet
File Name mobile-ffmpeg/colorspace.c
Method displayHSVColorRange(l_int32 hval,

```
....
1403.       huedelta = (l_int32)((l_float32)huehw / (l_float32)nsamp);
```

Divide By Zero\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=429
Status New

The application performs an illegal operation in displayHSVColorRange, in mobile-ffmpeg/colorspace.c. In line 1378, the program attempts to divide by nsamp, 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 nsamp in displayHSVColorRange of mobile-ffmpeg/colorspace.c, at line 1378.

	Source	Destination
File	mobile-ffmpeg/colorspace.c	mobile-ffmpeg/colorspace.c
Line	1404	1404
Object	nsamp	nsamp

Code Snippet
File Name mobile-ffmpeg/colorspace.c
Method displayHSVColorRange(l_int32 hval,

```
....
1404.       satdelta = (l_int32)((l_float32)sathw / (l_float32)nsamp);
```

Divide By Zero\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=430
Status New

The application performs an illegal operation in pixCentroid8, in mobile-ffmpeg/compare.c. In line 2412, the program attempts to divide by sumv, 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 sumv in pixCentroid8 of mobile-ffmpeg/compare.c, at line 2412.

	Source	Destination
File	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	2454	2454
Object	sumv	sumv

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixCentroid8(PIX *pixs,

```
....
2454.          *pcx = sumx / sumv;
```

Divide By Zero\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=431
Status	New

The application performs an illegal operation in pixCentroid8, in mobile-ffmpeg/compare.c. In line 2412, the program attempts to divide by sumv, 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 sumv in pixCentroid8 of mobile-ffmpeg/compare.c, at line 2412.

	Source	Destination
File	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	2455	2455
Object	sumv	sumv

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixCentroid8(PIX *pixs,

```
....
2455.          *pcy = sumy / sumv;
```

Divide By Zero\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=432
Status	New

The application performs an illegal operation in pixBlockconvTiled, in mobile-ffmpeg/convolve.c. In line 729, the program attempts to divide by nx, 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 nx in pixBlockconvTiled of mobile-ffmpeg/convolve.c, at line 729.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	761	761
Object	nx	nx

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method pixBlockconvTiled(PIX *pix,

```
....
761.        xrat = w / nx;
```

Divide By Zero\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=433
Status New

The application performs an illegal operation in pixBlockconvTiled, in mobile-ffmpeg/convolve.c. In line 729, the program attempts to divide by ny, 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 ny in pixBlockconvTiled of mobile-ffmpeg/convolve.c, at line 729.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	762	762
Object	ny	ny

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method pixBlockconvTiled(PIX *pix,

```
....
762.        yrat = h / ny;
```

Divide By Zero\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=434
Status New

The application performs an illegal operation in pixBlockconvTiled, in mobile-ffmpeg/convolve.c. In line 729, the program attempts to divide by BinaryExpr, 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 BinaryExpr in pixBlockconvTiled of mobile-ffmpeg/convolve.c, at line 729.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	764	764
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method pixBlockconvTiled(PIX *pix,

```
....
764.          nx = w / (wc + 2);
```

Divide By Zero\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=435
Status New

The application performs an illegal operation in pixBlockconvTiled, in mobile-ffmpeg/convolve.c. In line 729, the program attempts to divide by BinaryExpr, 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 BinaryExpr in pixBlockconvTiled of mobile-ffmpeg/convolve.c, at line 729.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	768	768
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method pixBlockconvTiled(PIX *pix,

```
....
768.          ny = h / (hc + 2);
```

Divide By Zero\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=436
Status New

The application performs an illegal operation in pixWindowedMean, in mobile-ffmpeg/convolve.c. In line 1067, the program attempts to divide by BinaryExpr, 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 BinaryExpr in pixWindowedMean of mobile-ffmpeg/convolve.c, at line 1067.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	1125	1125
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method pixWindowedMean(PIX *pixs,

```
....
1125.          norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=437
Status	New

The application performs an illegal operation in pixWindowedMeanSquare, in mobile-ffmpeg/convolve.c. In line 1184, the program attempts to divide by BinaryExpr, 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 BinaryExpr in pixWindowedMeanSquare of mobile-ffmpeg/convolve.c, at line 1184.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	1238	1238
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method pixWindowedMeanSquare(PIX *pixs,

```
....
1238.      norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=438
Status	New

The application performs an illegal operation in pixMeasureEdgeSmoothness, in mobile-ffmpeg/edge.c. In line 309, the program attempts to divide by CastExpr, 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 CastExpr in pixMeasureEdgeSmoothness of mobile-ffmpeg/edge.c, at line 309.

	Source	Destination
File	mobile-ffmpeg/edge.c	mobile-ffmpeg/edge.c
Line	359	359
Object	CastExpr	CastExpr

Code Snippet
File Name mobile-ffmpeg/edge.c
Method pixMeasureEdgeSmoothness(PIX *pixs,

```
....
359.              *pjpl = (l_float32)njumps / (l_float32)(n - 1);
```

Divide By Zero\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=439
Status New

The application performs an illegal operation in pixMeasureEdgeSmoothness, in mobile-ffmpeg/edge.c. In line 309, the program attempts to divide by CastExpr, 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 CastExpr in pixMeasureEdgeSmoothness of mobile-ffmpeg/edge.c, at line 309.

	Source	Destination
File	mobile-ffmpeg/edge.c	mobile-ffmpeg/edge.c
Line	361	361
Object	CastExpr	CastExpr

Code Snippet
File Name mobile-ffmpeg/edge.c
Method pixMeasureEdgeSmoothness(PIX *pixs,

```
....
361.              *pjspl = (l_float32)jumpsum / (l_float32)(n - 1);
```

Divide By Zero\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=440
Status New

The application performs an illegal operation in pixMeasureEdgeSmoothness, in mobile-ffmpeg/edge.c. In line 309, the program attempts to divide by CastExpr, 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 CastExpr in pixMeasureEdgeSmoothness of mobile-ffmpeg/edge.c, at line 309.

	Source	Destination
File	mobile-ffmpeg/edge.c	mobile-ffmpeg/edge.c
Line	367	367
Object	CastExpr	CastExpr

Code Snippet
File Name mobile-ffmpeg/edge.c
Method pixMeasureEdgeSmoothness(PIX *pixs,

```
....
367.          *prpl = (l_float32)nreversal / (l_float32)(n - 1);
```

Divide By Zero\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=441
Status	New

The application performs an illegal operation in numaGammaTRC, in mobile-ffmpeg/enhance.c. In line 369, the program attempts to divide by CastExpr, 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 CastExpr in numaGammaTRC of mobile-ffmpeg/enhance.c, at line 369.

	Source	Destination
File	mobile-ffmpeg/enhance.c	mobile-ffmpeg/enhance.c
Line	393	393
Object	CastExpr	CastExpr

Code Snippet
File Name mobile-ffmpeg/enhance.c
Method numaGammaTRC(l_float32 gamma,

```
....
393.          x = (l_float32)(i - minval) / (l_float32)(maxval -
minval);
```

Divide By Zero\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=442
Status	New

The application performs an illegal operation in pixDarkenGray, in mobile-ffmpeg/enhance.c. In line 2027, the program attempts to divide by satlimit, 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 satlimit in pixDarkenGray of mobile-ffmpeg/enhance.c, at line 2027.

	Source	Destination
File	mobile-ffmpeg/enhance.c	mobile-ffmpeg/enhance.c
Line	2068	2068
Object	satlimit	satlimit

Code Snippet
File Name mobile-ffmpeg/enhance.c
Method pixDarkenGray(PIX *pixd,

```
....
2068.              ratio = (l_float32)sat / (l_float32)satlimit;
```

Divide By Zero\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=443
Status New

The application performs an illegal operation in generatePtaHashBox, in mobile-ffmpeg/graphics.c. In line 405, the program attempts to divide by spacing, 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 spacing in generatePtaHashBox of mobile-ffmpeg/graphics.c, at line 405.

	Source	Destination
File	mobile-ffmpeg/graphics.c	mobile-ffmpeg/graphics.c
Line	439	439
Object	spacing	spacing

Code Snippet
File Name mobile-ffmpeg/graphics.c
Method generatePtaHashBox(BOX *box,

```
....
439.          n = 1 + bh / spacing;
```

Divide By Zero\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=444
Status New

The application performs an illegal operation in generatePtaHashBox, in mobile-ffmpeg/graphics.c. In line 405, the program attempts to divide by spacing, 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 spacing in generatePtaHashBox of mobile-ffmpeg/graphics.c, at line 405.

	Source	Destination
File	mobile-ffmpeg/graphics.c	mobile-ffmpeg/graphics.c
Line	447	447
Object	spacing	spacing

Code Snippet
File Name mobile-ffmpeg/graphics.c
Method generatePtaHashBox(BOX *box,

```
....
447.          n = 1 + bw / spacing;
```

Divide By Zero\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=445
Status	New

The application performs an illegal operation in generatePtaGrid, in mobile-ffmpeg/graphics.c. In line 722, the program attempts to divide by nx, 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 nx in generatePtaGrid of mobile-ffmpeg/graphics.c, at line 722.

	Source	Destination
File	mobile-ffmpeg/graphics.c	mobile-ffmpeg/graphics.c
Line	745	745
Object	nx	nx

Code Snippet
File Name mobile-ffmpeg/graphics.c
Method generatePtaGrid(l_int32 w,

```
....
745.      bx = (w + nx - 1) / nx;
```

Divide By Zero\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=446
Status	New

The application performs an illegal operation in generatePtaGrid, in mobile-ffmpeg/graphics.c. In line 722, the program attempts to divide by ny, 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 ny in generatePtaGrid of mobile-ffmpeg/graphics.c, at line 722.

	Source	Destination
File	mobile-ffmpeg/graphics.c	mobile-ffmpeg/graphics.c
Line	746	746
Object	ny	ny

Code Snippet
File Name mobile-ffmpeg/graphics.c
Method generatePtaGrid(l_int32 w,

```
....
746.      by = (h + ny - 1) / ny;
```

Divide By Zero\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=447
Status New

The application performs an illegal operation in pixRenderContours, in mobile-ffmpeg/graphics.c. In line 2619, the program attempts to divide by incr, 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 incr in pixRenderContours of mobile-ffmpeg/graphics.c, at line 2619.

	Source	Destination
File	mobile-ffmpeg/graphics.c	mobile-ffmpeg/graphics.c
Line	2670	2670
Object	incr	incr

Code Snippet
File Name mobile-ffmpeg/graphics.c
Method pixRenderContours(PIX *pixs,

```
....
2670.                    test = (val - startval) % incr;
```

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=1060095&projectid=60085&pathid=946
Status	New

The variable declared in output at mobile-ffmpeg/floor1.c in line 576 is not initialized when it is used by output at mobile-ffmpeg/floor1.c in line 576.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	590	700
Object	output	output

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int *floor1_fit(vorbis_block *vb,vorbis_look_floor1 *look,

```
....
590.    int *output=NULL;
....
700.      output=_vorbis_block_alloc(vb,sizeof(*output)*posts);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=947
Status	New

The variable declared in output at mobile-ffmpeg/floor1.c in line 731 is not initialized when it is used by output at mobile-ffmpeg/floor1.c in line 731.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	737	740
Object	output	output

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int *floor1_interpolate_fit(vorbis_block *vb,vorbis_look_floor1 *look,

```
....
737.    int *output=NULL;
....
740.      output=_vorbis_block_alloc(vb,sizeof(*output)*posts);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=948
Status	New

The variable declared in rgb at mobile-ffmpeg/jpegdec.c in line 258 is not initialized when it is used by rgb at mobile-ffmpeg/jpegdec.c in line 258.

	Source	Destination
File	mobile-ffmpeg/jpegdec.c	mobile-ffmpeg/jpegdec.c
Line	266	304
Object	rgb	rgb

Code Snippet
File Name mobile-ffmpeg/jpegdec.c
Method int ReadJPEG(const uint8_t* const data, size_t data_size,

```
....
266.    uint8_t* volatile rgb = NULL;
....
304.    stride = (int64_t)dinfo.output_width * dinfo.output_components *
sizeof(*rgb);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=949
Status	New

The variable declared in file_name at mobile-ffmpeg/makepng.c in line 1678 is not initialized when it is used by png_ptr at mobile-ffmpeg/makepng.c in line 770.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1681	774
Object	file_name	png_ptr

Code Snippet
File Name mobile-ffmpeg/makepng.c

Method	main(int argc, char **argv)

```
....
1681.     const char *file_name = NULL;
```

File Name	mobile-ffmpeg/makepng.c
Method	write_png(const char **name, FILE *fp, int color_type, int bit_depth,

```
....
774.     png_structp png_ptr =
png_create_write_struct(PNG_LIBPNG_VER_STRING,
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=950
Status	New

The variable declared in data at mobile-ffmpeg/makepng.c in line 1259 is not initialized when it is used by data at mobile-ffmpeg/makepng.c in line 1259.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1276	1282
Object	data	data

Code Snippet	
File Name	mobile-ffmpeg/makepng.c
Method	set_text(png_structp png_ptr, png_infop info_ptr, png_textp text,

```
....
1276.              png_bytep data = NULL;
....
1282.                 text->text = (png_charp)data;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=951
Status	New

The variable declared in endptr at mobile-ffmpeg/makepng.c in line 1098 is not initialized when it is used by data at mobile-ffmpeg/makepng.c in line 1259.

	Source	Destination

File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1100	1282
Object	endptr	data

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_fake(png_charp param, png_bytepp profile)

```
....
1100.     char *endptr = NULL;
```

File Name mobile-ffmpeg/makepng.c
Method set_text(png_structp png_ptr, png_infop info_ptr, png_textp text,

```
....
1282.                 text->text = (png_charp)data;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=952
Status	New

The variable declared in file at mobile-ffmpeg/makepng.c in line 1259 is not initialized when it is used by file at mobile-ffmpeg/makepng.c in line 1259.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1266	1269
Object	file	file

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method set_text(png_structp png_ptr, png_infop info_ptr, png_textp text,

```
....
1266.             png_bytep file = NULL;
....
1269.             text->text = (png_charp)file;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=953
Status	New

The variable declared in value at mobile-ffmpeg/tif_dirread.c in line 3574 is not initialized when it is used by value at mobile-ffmpeg/tif_dirread.c in line 3574.

	Source	Destination
File	mobile-ffmpeg/tif_dirread.c	mobile-ffmpeg/tif_dirread.c
Line	3920	3968
Object	value	value

Code Snippet
File Name mobile-ffmpeg/tif_dirread.c
Method TIFFReadDirectory(TIFF* tif)

```
....
3920.                                       uint16* value=NULL;
....
3968.                                             TIFFSetField(tif,dp-
>tdir_tag,value,value+incrementpersample,value+2*incrementpersample);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=954
Status	New

The variable declared in value at mobile-ffmpeg/tif_dirread.c in line 3574 is not initialized when it is used by value at mobile-ffmpeg/tif_dirread.c in line 3574.

	Source	Destination
File	mobile-ffmpeg/tif_dirread.c	mobile-ffmpeg/tif_dirread.c
Line	3920	3968
Object	value	value

Code Snippet
File Name mobile-ffmpeg/tif_dirread.c
Method TIFFReadDirectory(TIFF* tif)

```
....
3920.                                       uint16* value=NULL;
....
3968.                                             TIFFSetField(tif,dp-
>tdir_tag,value,value+incrementpersample,value+2*incrementpersample);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=955
Status	New

The variable declared in r at mobile-ffmpeg/tiff2pdf.c in line 1292 is not initialized when it is used by r at mobile-ffmpeg/tiff2pdf.c in line 1292.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1295	1554
Object	r	r

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_data(T2P* t2p, TIFF* input){

```
....
1295.       uint16* r = NULL;
....
1554.                           t2p->pdf_palette[(i*3)]  = (unsigned char)
(r[i]>>8);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=956
Status	New

The variable declared in g at mobile-ffmpeg/tiff2pdf.c in line 1292 is not initialized when it is used by g at mobile-ffmpeg/tiff2pdf.c in line 1292.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1296	1555
Object	g	g

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_data(T2P* t2p, TIFF* input){

```
....
1296.       uint16* g = NULL;
....
1555.                           t2p->pdf_palette[(i*3)+1]= (unsigned char)
(g[i]>>8);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=957
Status	New

The variable declared in b at mobile-ffmpeg/tiff2pdf.c in line 1292 is not initialized when it is used by b at mobile-ffmpeg/tiff2pdf.c in line 1292.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1297	1556
Object	b	b

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_data(T2P* t2p, TIFF* input){

```
....
1297.       uint16* b = NULL;
....
1556.                           t2p->pdf_palette[(i*3)+2]= (unsigned char)
(b[i]>>8);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=958
Status	New

The variable declared in sbc at mobile-ffmpeg/tiff2pdf.c in line 1944 is not initialized when it is used by sbc at mobile-ffmpeg/tiff2pdf.c in line 1944.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1946	1962
Object	sbc	sbc

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_size(T2P* t2p, TIFF* input){

```
....
1946.       uint64* sbc=NULL;
....
1962.                   t2p->tiff_datasize=(tmsize_t)sbc[0];
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=959
Status	New

The variable declared in sbc at mobile-ffmpeg/tiff2pdf.c in line 1944 is not initialized when it is used by sbc at mobile-ffmpeg/tiff2pdf.c in line 1944.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1946	1973
Object	sbc	sbc

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_size(T2P* t2p, TIFF* input){

```
....
1946.       uint64* sbc=NULL;
....
1973.                   t2p->tiff_datasize=(tmsize_t)sbc[0];
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=960
Status	New

The variable declared in sbc at mobile-ffmpeg/tiff2pdf.c in line 1944 is not initialized when it is used by sbc at mobile-ffmpeg/tiff2pdf.c in line 1944.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1946	1988
Object	sbc	sbc

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_size(T2P* t2p, TIFF* input){

```
....
1946.       uint64* sbc=NULL;
....
1988.                       k = checkAdd64(k, sbc[i], t2p);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=961
Status	New

The variable declared in sbc at mobile-ffmpeg/tiff2pdf.c in line 1944 is not initialized when it is used by sbc at mobile-ffmpeg/tiff2pdf.c in line 1944.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	1946	2050
Object	sbc	sbc

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_size(T2P* t2p, TIFF* input){

```
....
1946.       uint64* sbc=NULL;
....
2050.                           k = checkAdd64(k, sbc[i], t2p);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=962
Status	New

The variable declared in tbc at mobile-ffmpeg/tiff2pdf.c in line 2089 is not initialized when it is used by tbc at mobile-ffmpeg/tiff2pdf.c in line 2089.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	2091	2115
Object	tbc	tbc

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method void t2p_read_tiff_size_tile(T2P* t2p, TIFF* input, ttile_t tile){

```
....
2091.       uint64* tbc = NULL;
....
2115.                   k=tbc[tile];
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=963
Status	New

The variable declared in buffer at mobile-ffmpeg/tiff2pdf.c in line 2813 is not initialized when it is used by buffer at mobile-ffmpeg/tiff2pdf.c in line 2813.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	2817	3121
Object	buffer	buffer

Code Snippet

File Name mobile-ffmpeg/tiff2pdf.c

Method tsize_t t2p_readwrite_pdf_image_tile(T2P* t2p, TIFF* input, TIFF* output, ttile_t tile){

```
....
2817.       unsigned char* buffer=NULL;
....
3121.                           (tdata_t)buffer,
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=964
Status	New

The variable declared in buffer at mobile-ffmpeg/tiff2pdf.c in line 2813 is not initialized when it is used by buffer at mobile-ffmpeg/tiff2pdf.c in line 2813.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	2817	3105
Object	buffer	buffer

Code Snippet

File Name mobile-ffmpeg/tiff2pdf.c

Method tsize_t t2p_readwrite_pdf_image_tile(T2P* t2p, TIFF* input, TIFF* output, ttile_t tile){

```
....
2817.       unsigned char* buffer=NULL;
....
3105.                           (tdata_t)buffer,
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=965
Status	New

The variable declared in buffer at mobile-ffmpeg/tiff2pdf.c in line 2813 is not initialized when it is used by buffer at mobile-ffmpeg/tiff2pdf.c in line 2813.

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	2817	3098
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_readwrite_pdf_image_tile(T2P* t2p, TIFF* input, TIFF* output, ttile_t tile){

```
....
2817.       unsigned char* buffer=NULL;
....
3098.                           (tdata_t)buffer,
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=966
Status	New

The variable declared in mmvar at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by cvt_deltas at mobile-ffmpeg/ttgxvar.c in line 3194.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	3421
Object	mmvar	cvt_deltas

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3421.             cvt_deltas[j] = old_cvt_delta + FT_MulFix( deltas[j],
apply );
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=967
Status	New

The variable declared in mmvar at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by cvt_deltas at mobile-ffmpeg/ttgxvar.c in line 3194.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	3463
Object	mmvar	cvt_deltas

Code Snippet

File Name mobile-ffmpeg/ttgxvar.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3463.             cvt_deltas[pindex] = old_cvt_delta + FT_MulFix(
deltas[j], apply );
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=968
Status	New

The variable declared in mmvar at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by cvt at mobile-ffmpeg/ttgxvar.c in line 3194.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	3430
Object	mmvar	cvt

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c
Method tt_face_vary_cvt(TT_Face face,

```
....
3430.                           ( FT_fdot6ToFixed( face->cvt[j] ) +
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=969
Status	New

The variable declared in mmvar at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by cvt at mobile-ffmpeg/ttgxvar.c in line 3194.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	3472
Object	mmvar	cvt

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c
Method tt_face_vary_cvt(TT_Face face,

```
....
3472.                          ( FT_fdot6ToFixed( face->cvt[pindex] ) +
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=970
Status	New

The variable declared in mmvar at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by mmvar at mobile-ffmpeg/ttgxvar.c in line 2036.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	2213
Object	mmvar	mmvar

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.      FT_MM_Var*           mmvar = NULL;
....
2213.          (FT_UShort*)( (char*)mmvar + mmvar_size );
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=971
Status	New

The variable declared in pCtx at mobile-ffmpeg/DecUT_ParseSyntax.cpp in line 67 is not initialized when it is used by pCtx at mobile-ffmpeg/DecUT_ParseSyntax.cpp in line 67.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	78	67
Object	pCtx	pCtx

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method void UninitDecoder (PWelsDecoderContext& pCtx) {

```
....
78.       pCtx = NULL;
....
67.   void UninitDecoder (PWelsDecoderContext& pCtx) {
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=972
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 276 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	289	605
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
289.     d->__nextchar = NULL;
```

File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
605.           d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=973
Status	New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	416	605
Object	optarg	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
416.    d->optarg = NULL;
....
605.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=974
Status New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1082	605
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1082.       d->__nextchar = NULL;
....
605.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=975
Status New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1096	605
Object	optarg	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1096.              d->optarg = NULL;
....
605.           d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=976
Status New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1097	605
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1097.            d->__nextchar = NULL;
....
605.           d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=977
Status New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1152	605
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1152.           d->__nextchar = NULL;
....
605.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=978
Status New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 276 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	289	722
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
289.    d->__nextchar = NULL;
```

File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
722.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 34:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=979
Status	New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	416	722
Object	optarg	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
416.    d->optarg = NULL;
....
722.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=980
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1082	722
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1082.       d->__nextchar = NULL;
....
722.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 36:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=981
Status	New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1096	722
Object	optarg	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1096.             d->optarg = NULL;
....
722.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=982
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1097	722
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1097.           d->__nextchar = NULL;
....
722.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 38:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=983
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1152	722
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1152.           d->__nextchar = NULL;
....
722.          d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=984
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 276 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	289	675
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
289.    d->__nextchar = NULL;
```

File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
675.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=985
Status	New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	416	675
Object	optarg	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
416.    d->optarg = NULL;
....
675.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=986
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1082	675
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1082.       d->__nextchar = NULL;
....
675.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=987
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1097	675
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1097.           d->__nextchar = NULL;
....
675.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=988
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1152	675
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1152.           d->__nextchar = NULL;
....
675.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=989
Status	New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1096	675
Object	optarg	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1096.             d->optarg = NULL;
....
675.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=990
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 276 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	289	717
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
289.    d->__nextchar = NULL;
```

File Name mobile-ffmpeg/getopt.c

Method _getopt_internal_r (

```
....
717.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=991
Status	New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	416	717
Object	optarg	__nextchar

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method _getopt_internal_r (

```
....
416.    d->optarg = NULL;
....
717.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=992
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c

Line	1082	717
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1082.       d->__nextchar = NULL;
....
717.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=993
Status	New

The variable declared in optarg at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1096	717
Object	optarg	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1096.             d->optarg = NULL;
....
717.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=994
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination

File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1097	717
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1097.           d->__nextchar = NULL;
....
717.                d->__nextchar += strlen (d->__nextchar);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=995
Status	New

The variable declared in __nextchar at mobile-ffmpeg/getopt.c in line 399 is not initialized when it is used by __nextchar at mobile-ffmpeg/getopt.c in line 399.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1152	717
Object	__nextchar	__nextchar

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
1152.           d->__nextchar = NULL;
....
717.                d->__nextchar += strlen (d->__nextchar);
```

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=1060095&projectid=60085&pathid=533
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1207 of mobile-ffmpeg/abx.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1294	1294
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1294.           max     = max_A*ampl < max_B   ?   max_B   :   max_A*ampl;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=534
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1207 of mobile-ffmpeg/abx.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1300	1300
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1300.           max     = max_A < max_B/ampl   ?   max_B/ampl   :   max_A;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=535
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 649 of mobile-ffmpeg/frontend.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	660	660
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *format_duration_string(SF_INFO * sfinfo, char *string, int string_size)

```
....
660.          minutes = (seconds / 60);
```

Integer Overflow\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=536
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 406 of mobile-ffmpeg/res0.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	439	439
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static long **_01class(vorbis_block *vb,vorbis_look_residue *vl,

```
....
439.        ent*=scale;
```

Integer Overflow\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=537
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 525 of mobile-ffmpeg/abx.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	546	546
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void setup (int fdd, int samples, long freq)

```
....
546.      org = arg = freq;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=538
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 406 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	422	422
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method static int accumulate_fit(const float *flr,const float *mdct,

```
....
422.          xa  += i;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=539
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 406 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	424	424

Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method static int accumulate_fit(const float *flr,const float *mdct,

```
....
424.          x2a += i*i;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=540
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 406 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	426	426
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method static int accumulate_fit(const float *flr,const float *mdct,

```
....
426.          xya += i*quantized;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=541
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 406 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	429	429
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/floor1.c

Method	static int accumulate_fit(const float *flr,const float *mdct,

```
....
429.            xb  += i;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=542
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 406 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	431	431
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	mobile-ffmpeg/floor1.c
Method	static int accumulate_fit(const float *flr,const float *mdct,

```
....
431.            x2b += i*i;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=543
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 406 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	433	433
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	mobile-ffmpeg/floor1.c
Method	static int accumulate_fit(const float *flr,const float *mdct,

```
....
433.            xyb += i*quantized;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=544
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 576 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	682	682
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int *floor1_fit(vorbis_block *vb,vorbis_look_floor1 *look,

```
....
682.                        hineighbor[j]=i;
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=545
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 576 of mobile-ffmpeg/floor1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	687	687
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int *floor1_fit(vorbis_block *vb,vorbis_look_floor1 *look,

```
....
687.                        loneighbor[j]=i;
```

Integer Overflow\Path 14:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=546
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 38 of mobile-ffmpeg/latticetune.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	151	151
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
151.            indexdiv*=bins;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=547
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 81 of mobile-ffmpeg/rdswitch.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/rdswitch.c	mobile-ffmpeg/rdswitch.c
Line	109	109
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/rdswitch.c
Method read_quant_tables(j_compress_ptr cinfo, char *filename, boolean force_baseline)

```
....
109.      table[0] = (unsigned int)val;
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=548
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 81 of mobile-ffmpeg/rdswitch.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/rdswitch.c	mobile-ffmpeg/rdswitch.c
Line	116	116
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/rdswitch.c
Method read_quant_tables(j_compress_ptr cinfo, char *filename, boolean force_baseline)

```
....
116.        table[i] = (unsigned int)val;
```

Integer Overflow\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=549
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 6002 of mobile-ffmpeg/tif_dirread.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tif_dirread.c	mobile-ffmpeg/tif_dirread.c
Line	6044	6044
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/tif_dirread.c
Method int _TIFFPartialReadStripArray(TIFF* tif, TIFFDirEntry* dirent,

```
....
6044.      sizeofvalint = (int)(sizeofval);
```

Integer Overflow\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=550
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 6002 of mobile-ffmpeg/tif_dirread.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tif_dirread.c	mobile-ffmpeg/tif_dirread.c
Line	6101	6101
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/tif_dirread.c
Method int _TIFFPartialReadStripArray(TIFF* tif, TIFFDirEntry* dirent,

```
....
6101.      iStartBefore = -(int)((nOffset - nOffsetStartPage) /
sizeofval);
```

Integer Overflow\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=551
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 59 of mobile-ffmpeg/tiff2dib.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tiff2dib.c	mobile-ffmpeg/tiff2dib.c
Line	93	93
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/tiff2dib.c
Method HDIB LoadTIFFinDIB(LPSTR lpFileName)

```
....
93.      SamplePerPixel = (int) (LineSize/imageWidth);
```

Integer Overflow\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=552
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 59 of mobile-ffmpeg/tiff2dib.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tiff2dib.c	mobile-ffmpeg/tiff2dib.c

Line	96	96
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/tiff2dib.c
Method HDIB LoadTIFFinDIB(LPSTR lpFileName)

```
....
96.      Align = 4 - (LineSize % 4);
```

Integer Overflow\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=553
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 397 of mobile-ffmpeg/transcoder_example.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	446	446
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int theora_transcode_bufferin(TC_INSTANCE *ttc, int isKeyFrame, char * bytes, int bytecount){

```
....
446.      frac_bits=(int)(total_bits&31);
```

Integer Overflow\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=554
Status New

A variable of a larger data type, seconds, is being assigned to a smaller data type, in 609 of mobile-ffmpeg/transcoder_example.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	889	889

Object	seconds	seconds

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
889.          int seconds=(long)timebase%60;
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=555
Status	New

A variable of a larger data type, minutes, is being assigned to a smaller data type, in 609 of mobile-ffmpeg/transcoder_example.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	890	890
Object	minutes	minutes

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
890.          int minutes=((long)timebase/60)%60;
```

Integer Overflow\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=556
Status	New

A variable of a larger data type, hours, is being assigned to a smaller data type, in 609 of mobile-ffmpeg/transcoder_example.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	891	891
Object	hours	hours

Code Snippet	
File Name	mobile-ffmpeg/transcoder_example.c
Method	int main(int argc,char *argv[]){

```
....
891.          int hours=(long)timebase/3600;
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=557
Status	New

A variable of a larger data type, index, is being assigned to a smaller data type, in 38 of mobile-ffmpeg/latticetune.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	148	148
Object	index	index

Code Snippet	
File Name	mobile-ffmpeg/latticetune.c
Method	int main(int argc,char *argv[]){

```
....
148.            int index= (j/indexdiv)%bins;
```

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=1060095&projectid=60085&pathid=910
Status	New

	Source	Destination
File	mobile-ffmpeg/tiffmedian.c	mobile-ffmpeg/tiffmedian.c
Line	421	421

Object	neW	neW

Code Snippet
File Name mobile-ffmpeg/tiffmedian.c
Method splitbox(Colorbox* ptr)

```
....
421.        register Colorbox *new;
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=911
Status New

	Source	Destination
File	mobile-ffmpeg/utils.c	mobile-ffmpeg/utils.c
Line	102	102
Object	str	str

Code Snippet
File Name mobile-ffmpeg/utils.c
Method void _fail(const char *format, ...)

```
....
102.        vasprintf(&str, format, arg_ptr);
```

Memory Leak\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=912
Status New

	Source	Destination
File	mobile-ffmpeg/cli.c	mobile-ffmpeg/cli.c
Line	196	196
Object	opts	opts

Code Snippet
File Name mobile-ffmpeg/cli.c
Method cmdline_opts_t* cmdline_opts_parse(const kvz_api *const api, int argc, char *argv[])

```
....
196.    cmdline_opts_t *opts = calloc(1, sizeof(cmdline_opts_t));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=913
Status	New

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	567	567
Object	data	data

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static void filter_permute_state_run(filter_permute_state_t * state,

```
....
567.        unsigned char *data = malloc(len);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=914
Status	New

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	215	215
Object	new_str	new_str

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
215.        char *new_str = malloc (top + 1);
```

Memory Leak\Path 6:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=915
Status	New

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	61	61
Object	filename	filename

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
61.      char *filename=strdup(argv[1]);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=916
Status	New

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1572	1572
Object	bar	bar

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method strstash(png_const_charp foo)

```
....
1572.        png_charp bar = malloc(strlen(foo)+1);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=917
Status	New

	Source	Destination
File	mobile-ffmpeg/cli.c	mobile-ffmpeg/cli.c
Line	237	237

Object	input	input

Code Snippet
File Name mobile-ffmpeg/cli.c
Method cmdline_opts_t* cmdline_opts_parse(const kvz_api *const api, int argc, char *argv[])

```
....
237.        opts->input = strdup(optarg);
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=918
Status New

	Source	Destination
File	mobile-ffmpeg/cli.c	mobile-ffmpeg/cli.c
Line	244	244
Object	output	output

Code Snippet
File Name mobile-ffmpeg/cli.c
Method cmdline_opts_t* cmdline_opts_parse(const kvz_api *const api, int argc, char *argv[])

```
....
244.        opts->output = strdup(optarg);
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=919
Status New

	Source	Destination
File	mobile-ffmpeg/cli.c	mobile-ffmpeg/cli.c
Line	251	251
Object	debug	debug

Code Snippet
File Name mobile-ffmpeg/cli.c
Method cmdline_opts_t* cmdline_opts_parse(const kvz_api *const api, int argc, char *argv[])

```
....
251.        opts->debug = strdup(optarg);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=920
Status	New

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1538	1538
Object	job_pids	job_pids

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method int main(int argc, const char *argv[])

```
....
1538.             job_pids = calloc(sizeof(int), job_limit);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=921
Status	New

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	829	829
Object	data	data

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static gnutls_datum_t db_fetch(void *dbf, gnutls_datum_t key)

```
....
829.        t.data = malloc(saved_data.size);
```

Memory Leak\Path 13:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=922
Status	New

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	845	845
Object	data	data

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int db_store(void *dbf, gnutls_datum_t key, gnutls_datum_t data)

```
....
845.        saved_data.data = malloc(data.size);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=923
Status	New

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	324	324
Object	__getopt_nonoption_flags	__getopt_nonoption_flags

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
324.              __getopt_nonoption_flags =
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=924
Status	New

	Source	Destination
File	mobile-ffmpeg/jpegdec.c	mobile-ffmpeg/jpegdec.c
Line	132	132

Object	bytes	bytes

Code Snippet
File Name mobile-ffmpeg/jpegdec.c
Method static int StoreICCP(j_decompress_ptr dinfo, MetadataPayload* const iccp) {

```
....
132.    iccp->bytes = (uint8_t*)malloc(total_size);
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=925
Status New

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	89	89
Object	encoder	encoder

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
89.    encoder = calloc(1, sizeof(kvz_encoder));
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=926
Status New

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	112	112
Object	states	states

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
112.    encoder->states = calloc(encoder->num_encoder_states,
sizeof(encoder_state_t));
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=927
Status	New

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	69	69
Object	name	name

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
69.         name=strdup(filename);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=928
Status	New

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	71	71
Object	name	name

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
71.         name=strdup(filename);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=929
Status	New

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1465	1465
Object	cip	cip

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method make_insert(png_const_charp what,

```
....
1465.     cip = malloc(offsetof(chunk_insert,parameters) +
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=930
Status	New

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1589	1589
Object	bar	bar

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method strstash_list(const png_const_charp *text)

```
....
1589.     result = bar = malloc(foo+1);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=931
Status	New

	Source	Destination
File	mobile-ffmpeg/sign-verify-ext.c	mobile-ffmpeg/sign-verify-ext.c

Line	97	97
Object	userdata	userdata

Code Snippet
File Name mobile-ffmpeg/sign-verify-ext.c
Method static gnutls_privkey_t load_virt_privkey(const gnutls_datum_t *txtkey, gnutls_pk_algorithm_t pk)

```
....
97.   userdata = calloc(1, sizeof(struct key_cb_data));
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=932
Status New

	Source	Destination
File	mobile-ffmpeg/test_opus_encode.c	mobile-ffmpeg/test_opus_encode.c
Line	368	368
Object	enccpy	enccpy

Code Snippet
File Name mobile-ffmpeg/test_opus_encode.c
Method int run_test1(int no_fuzz)

```
....
368.        enccpy=(OpusEncoder *)malloc(opus_encoder_get_size(2));
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=933
Status New

	Source	Destination
File	mobile-ffmpeg/utils.c	mobile-ffmpeg/utils.c
Line	277	277
Object	p	p

Code Snippet
File Name mobile-ffmpeg/utils.c
Method static void append(const char *file)

```
....
277.        p = calloc(1, sizeof(*p));
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=934
Status	New

	Source	Destination
File	mobile-ffmpeg/test_opus_encode.c	mobile-ffmpeg/test_opus_encode.c
Line	352	352
Object	dec_err	dec_err

Code Snippet
File Name mobile-ffmpeg/test_opus_encode.c
Method int run_test1(int no_fuzz)

```
....
352.     dec_err[0]=(OpusDecoder *)malloc(opus_decoder_get_size(2));
```

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=1060095&projectid=60085&pathid=873
Status	New

Calling free() (line 947) on a variable that was not dynamically allocated (line 947) in file mobile-ffmpeg/abx.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	976	976
Object	name_q	name_q

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
976.      free (name_q);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=874
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file mobile-ffmpeg/getopt.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	598	598
Object	buf	buf

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
598.                free (buf);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=875
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file mobile-ffmpeg/getopt.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	670	670
Object	buf	buf

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
670.                    free (buf);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=876
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file mobile-ffmpeg/getopt.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	786	786
Object	buf	buf

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
786.                free (buf);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=877
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file mobile-ffmpeg/getopt.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	852	852
Object	buf	buf

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
852.              free (buf);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=878
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file mobile-ffmpeg/getopt.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	903	903
Object	buf	buf

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
903.                  free (buf);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=879
Status	New

Calling free() (line 399) on a variable that was not dynamically allocated (line 399) in file mobile-ffmpeg/getopt.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	976	976
Object	buf	buf

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
976.                    free (buf);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=880
Status	New

Calling free() (line 3066) on a variable that was not dynamically allocated (line 3066) in file mobile-ffmpeg/localename.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	3090	3090
Object	found	found

Code Snippet
File Name mobile-ffmpeg/localename.c
Method freelocale (locale_t locale)

```
....
3090.       free (found);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=881
Status	New

Calling free() (line 319) on a variable that was not dynamically allocated (line 319) in file mobile-ffmpeg/utils.c may result with a crash.

	Source	Destination
File	mobile-ffmpeg/utils.c	mobile-ffmpeg/utils.c
Line	330	330
Object	p	p

Code Snippet
File Name mobile-ffmpeg/utils.c
Method void delete_temp_files(void)

```
....
330.                free(p);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=882
Status	New

Calling free() (line 219) on a variable that was not dynamically allocated (line 219) in file mobile-ffmpeg/degradeimage.cpp may result with a crash.

	Source	Destination
File	mobile-ffmpeg/degradeimage.cpp	mobile-ffmpeg/degradeimage.cpp
Line	257	257
Object	im_coeffs	im_coeffs

Code Snippet
File Name mobile-ffmpeg/degradeimage.cpp
Method void GeneratePerspectiveDistortion(int width, int height, TRand* randomizer,

```
....
257.    free(im_coeffs);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=883
Status	New

Calling free() (line 219) on a variable that was not dynamically allocated (line 219) in file mobile-ffmpeg/degradeimage.cpp may result with a crash.

	Source	Destination
File	mobile-ffmpeg/degradeimage.cpp	mobile-ffmpeg/degradeimage.cpp
Line	258	258
Object	box_coeffs	box_coeffs

Code Snippet
File Name mobile-ffmpeg/degradeimage.cpp
Method void GeneratePerspectiveDistortion(int width, int height, TRand* randomizer,

```
....
258.    free(box_coeffs);
```

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=1060095&projectid=60085&pathid=522
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2438 of mobile-ffmpeg/tiff2ps.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tiff2ps.c	mobile-ffmpeg/tiff2ps.c
Line	2481	2481
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/tiff2ps.c
Method PSDataColorContig(FILE* fd, TIFF* tif, uint32 w, uint32 h, int nc)

```
....
2481.                        case 4: c = *cp++ + adjust; PUTHEX(c,fd);
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=523
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2438 of mobile-ffmpeg/tiff2ps.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tiff2ps.c	mobile-ffmpeg/tiff2ps.c
Line	2482	2482
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	mobile-ffmpeg/tiff2ps.c
Method	PSDataColorContig(FILE* fd, TIFF* tif, uint32 w, uint32 h, int nc)

```
....
2482.                           case 3: c = *cp++ + adjust; PUTHEX(c,fd);
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=524
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2438 of mobile-ffmpeg/tiff2ps.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tiff2ps.c	mobile-ffmpeg/tiff2ps.c
Line	2483	2483
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	mobile-ffmpeg/tiff2ps.c
Method	PSDataColorContig(FILE* fd, TIFF* tif, uint32 w, uint32 h, int nc)

```
....
2483.                           case 2: c = *cp++ + adjust; PUTHEX(c,fd);
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=525
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2438 of mobile-ffmpeg/tiff2ps.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tiff2ps.c	mobile-ffmpeg/tiff2ps.c
Line	2484	2484
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	mobile-ffmpeg/tiff2ps.c
Method	PSDataColorContig(FILE* fd, TIFF* tif, uint32 w, uint32 h, int nc)

```
....
2484.                          case 1: c = *cp++ + adjust; PUTHEX(c,fd);
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=526
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2613 of mobile-ffmpeg/tiff2ps.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/tiff2ps.c	mobile-ffmpeg/tiff2ps.c
Line	2713	2713
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/tiff2ps.c
Method PSDataBW(FILE* fd, TIFF* tif, uint32 w, uint32 h)

```
....
2713.                              c = *cp++ + adjust; PUTHEX(c,fd);
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=527
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 42 of mobile-ffmpeg/ulaw_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/ulaw_test.c	mobile-ffmpeg/ulaw_test.c
Line	112	112
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/ulaw_test.c
Method main (void)

```
....
112.              ulaw_buffer [k] = k & 0xFF ;
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=528
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 186 of mobile-ffmpeg/ulaw_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/ulaw_test.c	mobile-ffmpeg/ulaw_test.c
Line	220	220
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/ulaw_test.c
Method unsigned char ulaw_encode (int sample)

```
....
220.        ulawbyte = ~ (sign | (exponent << 4) | mantissa) ;
```

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=1060095&projectid=60085&pathid=516
Status	New

The function len in mobile-ffmpeg/dtls-stress.c at line 562 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	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	567	567
Object	len	len

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static void filter_permute_state_run(filter_permute_state_t * state,

```
....
567.        unsigned char *data = malloc(len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=517
Status	New

The function total_size in mobile-ffmpeg/jpegdec.c at line 62 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	mobile-ffmpeg/jpegdec.c	mobile-ffmpeg/jpegdec.c
Line	132	132
Object	total_size	total_size

Code Snippet
File Name mobile-ffmpeg/jpegdec.c
Method static int StoreICCP(j_decompress_ptr dinfo, MetadataPayload* const iccp) {

```
....
132.    iccp->bytes = (uint8_t*)malloc(total_size);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=518
Status	New

The function rowbytes in mobile-ffmpeg/makepng.c at line 770 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	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	955	955
Object	rowbytes	rowbytes

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method write_png(const char **name, FILE *fp, int color_type, int bit_depth,

```
....
955.            row = malloc(rowbytes);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=519
Status	New

The function foo in mobile-ffmpeg/makepng.c at line 1580 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	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1589	1589
Object	foo	foo

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method strstash_list(const png_const_charp *text)

```
....
1589.      result = bar = malloc(foo+1);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=520
Status	New

The function total in mobile-ffmpeg/makepng.c at line 996 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	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1043	1043
Object	total	total

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
1043.                    png_bytep data = malloc((total+3)&~3);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=521
Status	New

The function size in mobile-ffmpeg/localename.c at line 2677 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	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	2690	2690
Object	size	size

Code Snippet
File Name mobile-ffmpeg/localename.c
Method struniq (const char *string)

```
....
2690.      malloc (FLEXSIZEOF (struct struniq_hash_node, contents,
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=1060095&projectid=60085&pathid=940
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	182	229
Object	shuffle_len	shuffle

Code Snippet
File Name mobile-ffmpeg/abx.c
Method size_t shuffle_len;

```
....
182.  size_t          shuffle_len;
```

File Name mobile-ffmpeg/abx.c

Method int fft (compl* fn, const size_t newlen)

```
....
229.                  shuffle [shuffle_len] [1] = j;
```

Use of Uninitialized Variable\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=941
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	182	228
Object	shuffle_len	shuffle

Code Snippet
File Name mobile-ffmpeg/abx.c
Method size_t shuffle_len;

```
....
182.  size_t          shuffle_len;
```

File Name mobile-ffmpeg/abx.c

Method int fft (compl* fn, const size_t newlen)

```
....
228.                  shuffle [shuffle_len] [0] = i;
```

Use of Uninitialized Variable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=942
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	182	230
Object	shuffle_len	shuffle_len

Code Snippet
File Name mobile-ffmpeg/abx.c
Method size_t shuffle_len;

```
....
182.  size_t          shuffle_len;
```

File Name mobile-ffmpeg/abx.c

Method int fft (compl* fn, const size_t newlen)

```
....
230.                  shuffle_len++;
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=943
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	182	267
Object	shuffle_len	shuffle_len

Code Snippet
File Name mobile-ffmpeg/abx.c
Method size_t shuffle_len;

```
....
182.  size_t          shuffle_len;
```

File Name mobile-ffmpeg/abx.c

Method int fft (compl* fn, const size_t newlen)

```
....
267.      for ( k = 0; k < shuffle_len; k++ ) {
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=944
Status	New

	Source	Destination
File	mobile-ffmpeg/tiff2dib.c	mobile-ffmpeg/tiff2dib.c
Line	74	112
Object	lpBits	lpBits

Code Snippet
File Name mobile-ffmpeg/tiff2dib.c
Method HDIB LoadTIFFinDIB(LPSTR lpFileName)

```
....
74.      char          *lpBits;
....
112.      if (lpBits)
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=945
Status	New

	Source	Destination
File	mobile-ffmpeg/test_opus_encode.c	mobile-ffmpeg/test_opus_encode.c
Line	117	140
Object	frame_size_enum	frame_size_enum

Code Snippet
File Name mobile-ffmpeg/test_opus_encode.c
Method int get_frame_size_enum(int frame_size, int sampling_rate)

```
....
117.     int frame_size_enum;
....
140.     return frame_size_enum;
```

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=1060095&projectid=60085&pathid=529
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1016 of mobile-ffmpeg/abx.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1069	1069
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/abx.c
Method double cross_analyze (const stereo_t* p1, const stereo_t *p2, size_t len)

```
....
1069.               P1 [i][0] = tmp1;
```

Float Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=530
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1016 of mobile-ffmpeg/abx.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1083	1083
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/abx.c
Method double cross_analyze (const stereo_t* p1, const stereo_t *p2, size_t len)

```
....
1083.               P1 [i][0] = a0*b0 - a1*b1;
```

Float Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=531
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1016 of mobile-ffmpeg/abx.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1084	1084
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/abx.c
Method double cross_analyze (const stereo_t* p1, const stereo_t *p2, size_t len)

```
....
1084.               P1 [i][1] = a0*b1 + a1*b0;
```

Float Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=532
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1016 of mobile-ffmpeg/abx.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1070	1070
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/abx.c
Method double cross_analyze (const stereo_t* p1, const stereo_t *p2, size_t len)

```
....
1070.               P2 [i][0] = tmp2;
```

Short Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Short Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Short Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=558
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 115 of mobile-ffmpeg/headerless_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/headerless_test.c	mobile-ffmpeg/headerless_test.c
Line	125	125
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/headerless_test.c
Method old_test (void)

```
....
125.              buffer [k] = k ;
```

Short Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=559
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 55 of mobile-ffmpeg/headerless_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/headerless_test.c	mobile-ffmpeg/headerless_test.c
Line	66	66
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/headerless_test.c
Method headerless_test (const char * filename, int format, int expected)

```
....
66.          buffer [k] = k ;
```

Short Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=560
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 205 of mobile-ffmpeg/multi_file_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/multi_file_test.c	mobile-ffmpeg/multi_file_test.c
Line	214	214
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/multi_file_test.c
Method write_file_at_end (int fd, int filetype, int channels, int file_num)

```
....
214.               data [k] = k ;
```

Short Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=561
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 42 of mobile-ffmpeg/ulaw_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	mobile-ffmpeg/ulaw_test.c	mobile-ffmpeg/ulaw_test.c
Line	66	66
Object	AssignExpr	AssignExpr

Code Snippet
File Name mobile-ffmpeg/ulaw_test.c
Method main (void)

```
....
66.         short_buffer [k] = k & 0xFFFF ;
```

Use of Uninitialized Pointer

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

Categories

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

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=936
Status	New

The variable declared in alloc_fmt at mobile-ffmpeg/doprnt.c in line 158 is not initialized when it is used by alloc_fmt at mobile-ffmpeg/doprnt.c in line 158.

	Source	Destination
File	mobile-ffmpeg/doprnt.c	mobile-ffmpeg/doprnt.c
Line	163	189
Object	alloc_fmt	alloc_fmt

Code Snippet
File Name mobile-ffmpeg/doprnt.c
Method __gmp_doprnt (const struct doprnt_funs_t *funs, void *data,

```
....
163.    char     *fmt, *alloc_fmt, *last_fmt, *this_fmt, *gmp_str;
....
189.    fmt = alloc_fmt;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=937
Status	New

The variable declared in mb at mobile-ffmpeg/tif_ojpeg.c in line 524 is not initialized when it is used by mb at mobile-ffmpeg/tif_ojpeg.c in line 524.

	Source	Destination
File	mobile-ffmpeg/tif_ojpeg.c	mobile-ffmpeg/tif_ojpeg.c

Line	529	575
Object	mb	mb

Code Snippet
File Name mobile-ffmpeg/tif_ojpeg.c
Method OJPEGVSetField(TIFF* tif, uint32 tag, va_list ap)

```
....
529.        uint64* mb;
....
575.                                sp->dctable_offset[n]=mb[n];
```

Use of Uninitialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=938
Status New

The variable declared in mb at mobile-ffmpeg/tif_ojpeg.c in line 524 is not initialized when it is used by mb at mobile-ffmpeg/tif_ojpeg.c in line 524.

	Source	Destination
File	mobile-ffmpeg/tif_ojpeg.c	mobile-ffmpeg/tif_ojpeg.c
Line	529	560
Object	mb	mb

Code Snippet
File Name mobile-ffmpeg/tif_ojpeg.c
Method OJPEGVSetField(TIFF* tif, uint32 tag, va_list ap)

```
....
529.        uint64* mb;
....
560.                                sp->qtable_offset[n]=mb[n];
```

Use of Uninitialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=939
Status New

The variable declared in mb at mobile-ffmpeg/tif_ojpeg.c in line 524 is not initialized when it is used by mb at mobile-ffmpeg/tif_ojpeg.c in line 524.

	Source	Destination

File	mobile-ffmpeg/tif_ojpeg.c	mobile-ffmpeg/tif_ojpeg.c
Line	529	590
Object	mb	mb

Code Snippet
File Name mobile-ffmpeg/tif_ojpeg.c
Method OJPEGVSetField(TIFF* tif, uint32 tag, va_list ap)

```
....
529.        uint64* mb;
....
590.                                    sp->actable_offset[n]=mb[n];
```

Environment Injection

Query Path:
CPP\Cx\CPP Medium Threat\Environment Injection Version:0

Categories

OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description
Environment Injection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=827
Status	New

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	291
Object	argc	getenv

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

Environment Injection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=828
Status	New

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	291
Object	getenv	getenv

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

Environment Injection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=829
Status	New

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	291
Object	argv	getenv

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

Use of Hard coded Cryptographic Key

Query Path:
CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Hard coded Cryptographic Key\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=908
Status	New

The variable keyframe_frequency at line 609 of mobile-ffmpeg/transcoder_example.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	743	743
Object	keyframe_frequency	keyframe_frequency

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
743.    ti.keyframe_frequency=32768;
```

Use of Hard coded Cryptographic Key\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=909
Status	New

The variable keyframe_frequency_force at line 609 of mobile-ffmpeg/transcoder_example.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	744	744

Object	keyframe_frequency_force	keyframe_frequency_force

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
744.    ti.keyframe_frequency_force=32768;
```

Use After Free

Query Path:
CPP\Cx\CPP Medium Threat\Use After Free Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Use After Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=935
Status	New

The pointer i at mobile-ffmpeg/dtls-stress.c in line 356 is being used after it has been freed.

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	361	361
Object	data	i

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static void filter_permute_state_free_buffer(filter_permute_state_t * state)

```
....
361.                free(state->packets[i].data);
```

Wrong Memory Allocation

Query Path:
CPP\Cx\CPP Medium Threat\Wrong Memory Allocation Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description
Wrong Memory Allocation\Path 1:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1021
Status	New

The function malloc in mobile-ffmpeg/DecUT_ParseSyntax.cpp at line 172 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	194	194
Object	sizeof	malloc

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
194.    m_pCtx = (PWelsDecoderContext)malloc (sizeof
(SWelsDecoderContext));
```

Uncontrolled Recursion

Query Path:
CPP\Cx\CPP Medium Threat\Uncontrolled Recursion Version:1

Description

Uncontrolled Recursion\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2130
Status	New

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	3093	3093
Object	freelocale	freelocale

Code Snippet
File Name mobile-ffmpeg/localename.c
Method freelocale (locale_t locale)

```
....
3093.    freelocale (locale);
```

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=1060095&projectid=60085&pathid=1022
Status	New

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1261
Object	fscanf	fscanf

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1023
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2625	2625
Object	fscanf	fscanf

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2625.      if (fscanf(fp, "\nPixa Version %d\n", &version) != 1)
```

Improper Resource Access Authorization\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1024
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2629	2629
Object	fscanf	fscanf

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2629.       if (fscanf(fp, "Number of pix = %d\n", &n) != 1)
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1025
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2642	2642
Object	fscanf	fscanf

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2642.           if ((fscanf(fp, " pix[%d]: xres = %d, yres = %d\n",
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1026
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c

Line	3034	3034
Object	fscanf	fscanf

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaReadStream(FILE *fp)

```
....
3034.       if (fscanf(fp, "\nPixaa Version %d\n", &version) != 1)
```

Improper Resource Access Authorization\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1027
Status New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	3038	3038
Object	fscanf	fscanf

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaReadStream(FILE *fp)

```
....
3038.       if (fscanf(fp, "Number of pixa = %d\n", &n) != 1)
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1028
Status New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	3051	3051
Object	fscanf	fscanf

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaReadStream(FILE *fp)

```
....
3051.          if ((fscanf(fp, "\n\n --------------- pixa[%d] ----------
-----\n",
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1029
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	984	984
Object	header	header

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
984.      fread ( header, sizeof(*header),
sizeof(header)/sizeof(*header), fp );
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1030
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	988	988
Object	buff	buff

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
988.              *len = fread ( buff, sizeof(stereo_t), maxlen, fp );
```

Improper Resource Access Authorization\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1031
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	995	995
Object	buff	buff

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
995.              *len = fread ( buff, sizeof(sample_t), maxlen, fp );
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1032
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1001	1001
Object	buff	buff

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
1001.              *len = fread ( buff, sizeof(stereo_t), maxlen, fp );
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1033
Status	New

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp

Line	158	158
Object	pBuf	pBuf

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::DecoderBs (const char* sFileName) {

```
....
158.    ASSERT_EQ (fread (pBuf, 1, iFileSize, pH264File), (unsigned int)
iFileSize);
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1034
Status New

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	256	256
Object	pBuf	pBuf

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method bool DecoderParseSyntaxTest::DecodeBs (const char* sFileName, EDecCase eDecCase) {

```
....
256.    if ((fread (pBuf, 1, iFileSize, pH264File) != (unsigned int)
iFileSize)) {
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1035
Status New

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	324	324
Object	pBuf	pBuf

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp

Method	bool DecoderParseSyntaxTest::ParseBs (const char* sFileName, EDecCase eDecCase) {

```
....
324.    if (fread (pBuf, 1, iFileSize, pH264File) != (unsigned
int)iFileSize) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1036
Status	New

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	186	186
Object	buf	buf

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method BOOL png2pnm (FILE *png_file, FILE *pnm_file, FILE *alpha_file,

```
....
186.    ret = fread (buf, 1, 8, png_file);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1037
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	163	163
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
163.    ret=fread(buffer,1,4,test);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1038
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	180	180
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
180.        ret=fread(buffer,1,4,test);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1039
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	181	181
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
181.        ret=fread(buffer,1,4,test);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1040
Status	New

	Source	Destination

File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	186	186
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
186.          ret=fread(buffer,1,4,test);
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1041
Status New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	192	192
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
192.            ret=fread(buffer,1,20,test);
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1042
Status New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	214	214
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
214.              ret=fread(buffer,1,4,test);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1043
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	218	218
Object	buffer	buffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
218.                ret=fread(buffer,1,4,test);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1044
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	240	240
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
240.        ret=fread(buffer+i,1,1,test);
```

Improper Resource Access Authorization\Path 24:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1045
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	321	321
Object	readbuffer	readbuffer

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int fetch_and_process_audio(FILE *audio,ogg_page *audiopage,

```
....
321.        int bytesread=fread(readbuffer,1,toread*2*audio_ch,audio);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1046
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	525	525
Object	frame	frame

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int fetch_and_process_video(FILE *video,ogg_page *videopage,

```
....
525.          int ret=fread(frame,1,6,video);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1047
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	536	536

Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int fetch_and_process_video(FILE *video,ogg_page *videopage,

```
....
536.                if(fread(&c,1,1,video)&&c=='\n')break;
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1048
Status New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	544	544
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int fetch_and_process_video(FILE *video,ogg_page *videopage,

```
....
544.            ret=fread(&framelength, sizeof(int), 1, video);
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1049
Status New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	547	547
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int fetch_and_process_video(FILE *video,ogg_page *videopage,

```
....
547.          ret=fread(&keyframeflag, sizeof(int), 1, video);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1050
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	554	554
Object	vp3frame	vp3frame

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int fetch_and_process_video(FILE *video,ogg_page *videopage,

```
....
554.          ret=fread((char *) vp3frame[i], sizeof(char), framelength,
video);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1051
Status	New

	Source	Destination
File	mobile-ffmpeg/dtls-stress.c	mobile-ffmpeg/dtls-stress.c
Line	1261	1261
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/dtls-stress.c
Method static int run_tests_from_id_list(int childcount)

```
....
1261.       while ((ret = fscanf(stdin, "%i\n", &test_id)) > 0) {
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1052
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2625	2625
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2625.       if (fscanf(fp, "\nPixa Version %d\n", &version) != 1)
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1053
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2629	2629
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2629.       if (fscanf(fp, "Number of pix = %d\n", &n) != 1)
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1054
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c

Line	2643	2643
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2643.                &ignore, &xres, &yres)) != 3) {
```

Improper Resource Access Authorization\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1055
Status New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2643	2643
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2643.                &ignore, &xres, &yres)) != 3) {
```

Improper Resource Access Authorization\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1056
Status New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2643	2643
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadStream(FILE *fp)

```
....
2643.                &ignore, &xres, &yres)) != 3) {
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1057
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	3034	3034
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaReadStream(FILE *fp)

```
....
3034.      if (fscanf(fp, "\nPixaa Version %d\n", &version) != 1)
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1058
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	3038	3038
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaReadStream(FILE *fp)

```
....
3038.      if (fscanf(fp, "Number of pixa = %d\n", &n) != 1)
```

Improper Resource Access Authorization\Path 38:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1059
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	3052	3052
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaReadStream(FILE *fp)

```
....
3052.                       &ignore)) != 1) {
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1060
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	167	167
Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int sel (void)

```
....
167.          ret = read (0, &c, 1);
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1061
Status	New

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	557	557

Object	Address	Address

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int getchar_keyboard (keyboard_t* const k)

```
....
557.          ret = read (0, &c, 1);
```

Improper Resource Access Authorization\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1062
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1258	1258
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1258.          fprintf ( stderr, "Different sample frequencies currently
not supported\n");
```

Improper Resource Access Authorization\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1063
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1259	1259
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1259.          fprintf ( stderr, "A: %ld, B: %ld\n", freq1, freq2 );
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1064
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1268	1268
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1268.          fprintf ( stderr, "Delay Ch1 is %.4f samples\n", fshift
);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1065
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1269	1269
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1269.       fprintf ( stderr, "Delay Ch2 is %.4f samples\n",
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1066
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1275	1275
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1275.               fprintf ( stderr, "Delaying A by %d samples\n",
+shift);
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1067
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1281	1281
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1281.               fprintf ( stderr, "Delaying B by %d samples\n", -
shift);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1068
Status	New

	Source	Destination

File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	282	282
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void printnumber (long double x)

```
....
282.      if      ( x < 9.999995  ) fprintf ( stderr, "%7.5f",
(double)x );
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1069
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	283	283
Object	fprintf	fprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void printnumber (long double x)

```
....
283.      else if ( x < 99.99995  ) fprintf ( stderr, "%7.4f",
(double)x );
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1070
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	284	284
Object	fprintf	fprintf

Code Snippet

File Name	mobile-ffmpeg/abx.c
Method	void printnumber (long double x)

```
....
284.      else if ( x < 999.9995  ) fprintf ( stderr, "%7.3f",
(double)x );
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=1071
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	285	285
Object	fprintf	fprintf

Code Snippet

File Name	mobile-ffmpeg/abx.c
Method	void printnumber (long double x)

```
....
285.      else if ( x < 9999.995  ) fprintf ( stderr, "%7.2f",
(double)x );
```

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=1060095&projectid=60085&pathid=2253
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	469	469
Object	tmp	sizeof

Code Snippet

File Name	mobile-ffmpeg/abx.c
Method	int feed (int fd, const stereo_t* p, int len)

```
....
469.        if (len > sizeof(tmp)/sizeof(*tmp))
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2254
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	469	469
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed (int fd, const stereo_t* p, int len)

```
....
469.        if (len > sizeof(tmp)/sizeof(*tmp))
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2255
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	494	494
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
494.        if (len > sizeof(tmp)/sizeof(*tmp))
```

Sizeof Pointer Argument\Path 4:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2256
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	494	494
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
494.        if (len > sizeof(tmp)/sizeof(*tmp))
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2257
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	513	513
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
513.        if (len > sizeof(tmp)/sizeof(*tmp))
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2258
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c

Line	513	513
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
513.        if (len > sizeof(tmp)/sizeof(*tmp))
```

Sizeof Pointer Argument\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2259
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	970	970
Object	decoder	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
970.       for ( i = 0; i < sizeof(decoder)/sizeof(*decoder); i++ )
```

Sizeof Pointer Argument\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2260
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	970	970
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
970.      for ( i = 0; i < sizeof(decoder)/sizeof(*decoder); i++ )
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2261
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	970	970
Object	decoder	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
970.      for ( i = 0; i < sizeof(decoder)/sizeof(*decoder); i++ )
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2262
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	970	970
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
970.      for ( i = 0; i < sizeof(decoder)/sizeof(*decoder); i++ )
```

Sizeof Pointer Argument\Path 11:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2263
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	470	470
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed (int fd, const stereo_t* p, int len)

```
....
470.          len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2264
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	469	470
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed (int fd, const stereo_t* p, int len)

```
....
469.       if (len > sizeof(tmp)/sizeof(*tmp))
470.          len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2265
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c

Line	469	470
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed (int fd, const stereo_t* p, int len)

```
....
469.        if (len > sizeof(tmp)/sizeof(*tmp))
470.            len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2266
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	470	470
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed (int fd, const stereo_t* p, int len)

```
....
470.            len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2267
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	469	470
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed (int fd, const stereo_t* p, int len)

```
....
469.        if (len > sizeof(tmp)/sizeof(*tmp))
470.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2268
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	469	470
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed (int fd, const stereo_t* p, int len)

```
....
469.        if (len > sizeof(tmp)/sizeof(*tmp))
470.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2269
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	495	495
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
495.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 18:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2270
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	494	495
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
494.        if (len > sizeof(tmp)/sizeof(*tmp))
495.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2271
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	494	495
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
494.        if (len > sizeof(tmp)/sizeof(*tmp))
495.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2272
Status	New

	Source	Destination

File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	495	495
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
495.          len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2273
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	494	495
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
494.       if (len > sizeof(tmp)/sizeof(*tmp))
495.          len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2274
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	494	495
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c

Method	int feed2 (int fd, const stereo_t* p1, const stereo_t* p2, int len)

```
....
494.        if (len > sizeof(tmp)/sizeof(*tmp))
495.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2275
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	514	514
Object	tmp	sizeof

Code Snippet	
File Name	mobile-ffmpeg/abx.c
Method	int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
514.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2276
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	513	514
Object	tmp	sizeof

Code Snippet	
File Name	mobile-ffmpeg/abx.c
Method	int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
513.        if (len > sizeof(tmp)/sizeof(*tmp))
514.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2277
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	513	514
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
513.        if (len > sizeof(tmp)/sizeof(*tmp))
514.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2278
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	514	514
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
514.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=2279
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	513	514
Object	tmp	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
513.        if (len > sizeof(tmp)/sizeof(*tmp))
514.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2280
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	513	514
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int feedfac (int fd, const stereo_t* p1, const stereo_t* p2, int len, double fac1, double fac2)

```
....
513.        if (len > sizeof(tmp)/sizeof(*tmp))
514.           len = sizeof(tmp)/sizeof(*tmp);
```

Sizeof Pointer Argument\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2281
Status	New

	Source	Destination

File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1345	1345
Object	freq	sizeof

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method insert_hIST(png_structp png_ptr, png_infop info_ptr, int nparams,

```
....
1345.     memset(freq, 0, sizeof freq);
```

Sizeof Pointer Argument\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2282
Status New

	Source	Destination
File	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	567	567
Object	resbits	sizeof

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static int _01forward(oggpack_buffer *opb,

```
....
567.    memset(resbits,0,sizeof(resbits));
```

Sizeof Pointer Argument\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2283
Status New

	Source	Destination
File	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	568	568
Object	resvals	sizeof

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static int _01forward(oggpack_buffer *opb,

```
....
568.    memset(resvals,0,sizeof(resvals));
```

Sizeof Pointer Argument\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2284
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	984	984
Object	header	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
984.      fread ( header, sizeof(*header),
sizeof(header)/sizeof(*header), fp );
```

Sizeof Pointer Argument\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2285
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	984	984
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
984.      fread ( header, sizeof(*header),
sizeof(header)/sizeof(*header), fp );
```

Sizeof Pointer Argument\Path 34:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2286
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	984	984
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
984.      fread ( header, sizeof(*header),
sizeof(header)/sizeof(*header), fp );
```

Sizeof Pointer Argument\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2287
Status	New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	984	984
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
984.      fread ( header, sizeof(*header),
sizeof(header)/sizeof(*header), fp );
```

Sizeof Pointer Argument\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2288
Status	New

	Source	Destination

File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	1386	1386
Object	legacy_table	sizeof

Code Snippet
File Name mobile-ffmpeg/localename.c
Method gl_locale_name_canonicalize (char *name)

```
....
1386.         i2 = sizeof (legacy_table) / sizeof (legacy_entry);
```

Sizeof Pointer Argument\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2289
Status New

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	1410	1410
Object	langtag_table	sizeof

Code Snippet
File Name mobile-ffmpeg/localename.c
Method gl_locale_name_canonicalize (char *name)

```
....
1410.         i2 = sizeof (langtag_table) / sizeof (langtag_entry);
```

Sizeof Pointer Argument\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2290
Status New

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	1429	1429
Object	script_table	sizeof

Code Snippet
File Name mobile-ffmpeg/localename.c
Method gl_locale_name_canonicalize (char *name)

```
....
1429.         i2 = sizeof (script_table) / sizeof (script_entry);
```

Sizeof Pointer Argument\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2291
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	423	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
423.         (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2292
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	423	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
423.         (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2293
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	413	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
413.    image1_coord = (double *)aom_malloc(sizeof(*image1_coord) *
npoints * 2);
....
423.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2294
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	413	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
413.    image1_coord = (double *)aom_malloc(sizeof(*image1_coord) *
npoints * 2);
....
423.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 43:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2295
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	412	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
412.    corners2 = (double *)aom_malloc(sizeof(*corners2) * npoints *
2);
....
423.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2296
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	412	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
412.    corners2 = (double *)aom_malloc(sizeof(*corners2) * npoints *
2);
....
423.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2297

Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	419	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
419.           (int *)aom_malloc(sizeof(*motions->inlier_indices) *
npoints);
....
423.         (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2298
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	419	423
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac(const int *matched_points, int npoints,

```
....
419.           (int *)aom_malloc(sizeof(*motions->inlier_indices) *
npoints);
....
423.         (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2299
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	604	604
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac_double_prec(const double *matched_points, int npoints,

```
....
604.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2300
Status New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	604	604
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac_double_prec(const double *matched_points, int npoints,

```
....
604.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2301
Status New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	594	604
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac_double_prec(const double *matched_points, int npoints,

```
....
594.    image1_coord = (double *)aom_malloc(sizeof(*image1_coord) *
npoints * 2);
....
604.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

Sizeof Pointer Argument\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2302
Status	New

	Source	Destination
File	mobile-ffmpeg/ransac.c	mobile-ffmpeg/ransac.c
Line	594	604
Object	Pointer	sizeof

Code Snippet
File Name mobile-ffmpeg/ransac.c
Method static int ransac_double_prec(const double *matched_points, int npoints,

```
....
594.    image1_coord = (double *)aom_malloc(sizeof(*image1_coord) *
npoints * 2);
....
604.        (int *)aom_malloc(sizeof(*current_motion.inlier_indices) *
npoints);
```

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=1060095&projectid=60085&pathid=2593
Status	New

	Source	Destination

File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	142	142
Object	VTIME	VTIME

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void set (void)

```
....
142.      new_settings.c_cc[VTIME] = 0;
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2594
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	143	143
Object	VMIN	VMIN

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void set (void)

```
....
143.      new_settings.c_cc[VMIN]  = 1;
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2595
Status New

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	967	967
Object	j	j

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
967.      name_q[j] = '\0';
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2596
Status	New

	Source	Destination
File	mobile-ffmpeg/colorquant2.c	mobile-ffmpeg/colorquant2.c
Line	1542	1542
Object	histoindex	histoindex

Code Snippet
File Name mobile-ffmpeg/colorquant2.c
Method vboxGetAverageColor(L_BOX3D *vbox,

```
....
1542.                      histo[histoindex] = index;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2597
Status	New

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	828	828
Object	ln	ln

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int floor1_encode(oggpack_buffer *opb,vorbis_block *vb,

```
....
828.          post[ln]&=0x7fff;
```

Unchecked Array Index\Path 6:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2598
Status	New

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	829	829
Object	hn	hn

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int floor1_encode(oggpack_buffer *opb,vorbis_block *vb,

```
....
829.          post[hn]&=0x7fff;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2599
Status	New

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	257	257
Object	c	c

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *build_shortopt_string(char *shortstr, struct option *opts)

```
....
257.      shortstr[c] = '\0';
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2600
Status	New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	575	575

Object	dcount	dcount

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdToBinaryLineLow(l_uint32 *lined,

```
....
575.            lined[dcount] = dword;
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2601
Status New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	617	617
Object	dcount	dcount

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdToBinaryLineLow(l_uint32 *lined,

```
....
617.              lined[dcount] = dword;
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2602
Status New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	1457	1457
Object	sval1	sval1

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdTo2bppLow(l_uint32 *datad,

```
....
1457.              dval = (tab[sval1] << 6) | (tab[sval2] << 4) |
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2603
Status	New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	1457	1457
Object	sval2	sval2

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdTo2bppLow(l_uint32 *datad,

```
....
1457.              dval = (tab[sval1] << 6) | (tab[sval2] << 4) |
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2604
Status	New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	1458	1458
Object	sval3	sval3

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdTo2bppLow(l_uint32 *datad,

```
....
1458.                     (tab[sval3] << 2) | tab[sval4];
```

Unchecked Array Index\Path 13:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2605
Status	New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	1600	1600
Object	sval1	sval1

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdTo4bppLow(l_uint32 *datad,

```
....
1600.              dval = (tab[sval1] << 12) | (tab[sval2] << 8) |
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2606
Status	New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	1600	1600
Object	sval2	sval2

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdTo4bppLow(l_uint32 *datad,

```
....
1600.              dval = (tab[sval1] << 12) | (tab[sval2] << 8) |
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2607
Status	New

	Source	Destination
File	mobile-ffmpeg/grayquant.c	mobile-ffmpeg/grayquant.c
Line	1601	1601

Object	sval3	sval3

Code Snippet
File Name mobile-ffmpeg/grayquant.c
Method thresholdTo4bppLow(l_uint32 *datad,

```
....
1601.                    (tab[sval3] << 4) | tab[sval4];
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2608
Status New

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	122	122
Object	code	code

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
122.          hits[code]+=val;
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2609
Status New

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	2709	2709
Object	slot	slot

Code Snippet
File Name mobile-ffmpeg/localename.c
Method struniq (const char *string)

```
....
2709.    struniq_hash_table[slot] = new_node;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2610
Status	New

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	2958	2958
Object	slot	slot

Code Snippet
File Name mobile-ffmpeg/localename.c
Method newlocale (int category_mask, const char *name, locale_t base)

```
....
2958.          locale_hash_table[slot] = node;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2611
Status	New

	Source	Destination
File	mobile-ffmpeg/localename.c	mobile-ffmpeg/localename.c
Line	3052	3052
Object	slot	slot

Code Snippet
File Name mobile-ffmpeg/localename.c
Method duplocale (locale_t locale)

```
....
3052.          locale_hash_table[slot] = node;
```

Unchecked Array Index\Path 20:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2612
Status	New

	Source	Destination
File	mobile-ffmpeg/lossless_msa.c	mobile-ffmpeg/lossless_msa.c
Line	196	196
Object	ptemp_dst	ptemp_dst

Code Snippet
File Name mobile-ffmpeg/lossless_msa.c
Method int num_pixels, uint8_t* dst) {

```
....
196.      }
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2613
Status	New

	Source	Destination
File	mobile-ffmpeg/lossless_msa.c	mobile-ffmpeg/lossless_msa.c
Line	196	196
Object	ptemp_dst	ptemp_dst

Code Snippet
File Name mobile-ffmpeg/lossless_msa.c
Method int num_pixels, uint8_t* dst) {

```
....
196.      }
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2614
Status	New

	Source	Destination
File	mobile-ffmpeg/lossless_msa.c	mobile-ffmpeg/lossless_msa.c
Line	196	196

Object	ptemp_dst	ptemp_dst

Code Snippet
File Name mobile-ffmpeg/lossless_msa.c
Method int num_pixels, uint8_t* dst) {

```
....
196.      }
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2615
Status	New

	Source	Destination
File	mobile-ffmpeg/lossless_msa.c	mobile-ffmpeg/lossless_msa.c
Line	243	243
Object	ptemp_dst	ptemp_dst

Code Snippet
File Name mobile-ffmpeg/lossless_msa.c
Method int num_pixels, uint8_t* dst) {

```
....
243.      }
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2616
Status	New

	Source	Destination
File	mobile-ffmpeg/lossless_msa.c	mobile-ffmpeg/lossless_msa.c
Line	243	243
Object	ptemp_dst	ptemp_dst

Code Snippet
File Name mobile-ffmpeg/lossless_msa.c
Method int num_pixels, uint8_t* dst) {

```
....
243.       }
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2617
Status	New

	Source	Destination
File	mobile-ffmpeg/lossless_msa.c	mobile-ffmpeg/lossless_msa.c
Line	243	243
Object	ptemp_dst	ptemp_dst

Code Snippet
File Name mobile-ffmpeg/lossless_msa.c
Method int num_pixels, uint8_t* dst) {

```
....
243.       }
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2618
Status	New

	Source	Destination
File	mobile-ffmpeg/mul_fft.c	mobile-ffmpeg/mul_fft.c
Line	301	301
Object	n	n

Code Snippet
File Name mobile-ffmpeg/mul_fft.c
Method mpn_fft_add_sub_modF (mp_ptr A0, mp_ptr Ai, mp_srcptr tp, mp_size_t n)

```
....
301.     Ai[n] = x + c;
```

Unchecked Array Index\Path 27:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2619
Status	New

	Source	Destination
File	mobile-ffmpeg/mul_fft.c	mobile-ffmpeg/mul_fft.c
Line	306	306
Object	n	n

Code Snippet
File Name mobile-ffmpeg/mul_fft.c
Method mpn_fft_add_sub_modF (mp_ptr A0, mp_ptr Ai, mp_srcptr tp, mp_size_t n)

```
....
306.    A0[n] = c - x;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2620
Status	New

	Source	Destination
File	mobile-ffmpeg/pix2.c	mobile-ffmpeg/pix2.c
Line	626	626
Object	x	x

Code Snippet
File Name mobile-ffmpeg/pix2.c
Method setPixelLow(l_uint32 *line,

```
....
626.            line[x] = val;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2621
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	157	157

Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetGrayHistogram(PIX *pixs,

```
....
157.                    array[val] += 1.0;
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2622
Status New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	162	162
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetGrayHistogram(PIX *pixs,

```
....
162.                    array[val] += 1.0;
```

Unchecked Array Index\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2623
Status New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	167	167
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetGrayHistogram(PIX *pixs,

```
....
167.                    array[val] += 1.0;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2624
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	172	172
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetGrayHistogram(PIX *pixs,

```
....
172.                    array[val] += 1.0;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2625
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	256	256
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetGrayHistogramMasked(PIX *pixs,

```
....
256.                    array[val] += 1.0;
```

Unchecked Array Index\Path 34:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2626
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	328	328
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetGrayHistogramInRect(PIX *pixs,

```
....
328.              array[val] += 1.0;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2627
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	468	468
Object	rval	rval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogram(PIX *pixs,

```
....
468.                  rarray[rval] += 1.0;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2628
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	469	469

Object	gval	gval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogram(PIX *pixs,

```
....
469.                    garray[gval] += 1.0;
```

Unchecked Array Index\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2629
Status New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	470	470
Object	bval	bval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogram(PIX *pixs,

```
....
470.                    barray[bval] += 1.0;
```

Unchecked Array Index\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2630
Status New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	478	478
Object	rval	rval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogram(PIX *pixs,

```
....
478.                    rarray[rval] += 1.0;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2631
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	479	479
Object	gval	gval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogram(PIX *pixs,

```
....
479.                    garray[gval] += 1.0;
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2632
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	480	480
Object	bval	bval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogram(PIX *pixs,

```
....
480.                    barray[bval] += 1.0;
```

Unchecked Array Index\Path 41:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2633
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	585	585
Object	rval	rval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogramMasked(PIX *pixs,

```
....
585.                    rarray[rval] += 1.0;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2634
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	586	586
Object	gval	gval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogramMasked(PIX *pixs,

```
....
586.                    garray[gval] += 1.0;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2635
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	587	587

Object	bval	bval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogramMasked(PIX *pixs,

```
....
587.                        barray[bval] += 1.0;
```

Unchecked Array Index\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2636
Status New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	600	600
Object	rval	rval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogramMasked(PIX *pixs,

```
....
600.                        rarray[rval] += 1.0;
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2637
Status New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	601	601
Object	gval	gval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogramMasked(PIX *pixs,

```
....
601.                        garray[gval] += 1.0;
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2638
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	602	602
Object	bval	bval

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetColorHistogramMasked(PIX *pixs,

```
....
602.                        barray[bval] += 1.0;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2639
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	664	664
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetCmapHistogram(PIX *pixs,

```
....
664.                array[val] += 1.0;
```

Unchecked Array Index\Path 48:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2640
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	745	745
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetCmapHistogramMasked(PIX *pixs,

```
....
745.                    array[val] += 1.0;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2641
Status	New

	Source	Destination
File	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	816	816
Object	val	val

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixGetCmapHistogramInRect(PIX *pixs,

```
....
816.                array[val] += 1.0;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2642
Status	New

	Source	Destination
File	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	1218	1218

Object	irow	irow

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaDisplayTiledAndScaled(PIXA *pixa,

```
....
1218.               rowht[irow] = maxht;
```

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=1060095&projectid=60085&pathid=2480
Status	New

The testing method calls the sprintf function, at line 582 of mobile-ffmpeg/abx.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	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	723	723
Object	sprintf	sprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void testing (const stereo_t* A, const stereo_t* B, size_t len, long freq)

```
....
723.               sprintf ( message, "  B (Errors -%c dB)", (char)c );
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2481
Status	New

The testing method calls the sprintf function, at line 582 of mobile-ffmpeg/abx.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	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	738	738
Object	sprintf	sprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void testing (const stereo_t* A, const stereo_t* B, size_t len, long freq)

```
....
738.              sprintf ( message, "  B (Errors +%c dB)", c );
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2482
Status New

The readwave method calls the sprintf function, at line 947 of mobile-ffmpeg/abx.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	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	972	972
Object	sprintf	sprintf

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
972.              sprintf ( command, decoder[i].command, name_q );
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2483
Status New

The ccbaWriteSVGString method calls the snprintf function, at line 2560 of mobile-ffmpeg/ccbord.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	mobile-ffmpeg/ccbord.c	mobile-ffmpeg/ccbord.c
Line	2603	2603
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/ccbord.c
Method ccbaWriteSVGString(const char *filename,

```
....
2603.              snprintf(smallbuf, sizeof(smallbuf), "%0d,%0d", x,
y);
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2484
Status New

The pixBestCorrelation method calls the snprintf function, at line 3507 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	3574	3574
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixBestCorrelation(PIX *pix1,

```
....
3574.          snprintf(buf, sizeof(buf),
"/tmp/lept/comp/correl_%d.png",
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2485
Status New

The pixCompareGray method calls the snprintf function, at line 862 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	920	920
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixCompareGray(PIX *pix1,

```
....
920.          snprintf(buf, sizeof(buf),
"/tmp/lept/comp/compare_gray%d", index);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2486
Status New

The pixCompareGray method calls the snprintf function, at line 862 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	927	927
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixCompareGray(PIX *pix1,

```
....
927.          snprintf(buf, sizeof(buf),
"/tmp/lept/comp/compare_gray%d.png",
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2487
Status New

The pixCompareRGB method calls the snprintf function, at line 971 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	1051	1051
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixCompareRGB(PIX *pix1,

```
....
1051.          snprintf(buf, sizeof(buf),
"/tmp/lept/comp/compare_rgb%d", index);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2488
Status	New

The pixCompareRGB method calls the snprintf function, at line 971 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	1060	1060
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixCompareRGB(PIX *pix1,

```
....
1060.          snprintf(buf, sizeof(buf),
"/tmp/lept/comp/compare_rgb%d.png",
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2489
Status	New

The pixGenPhotoHistos method calls the snprintf function, at line 2245 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	2330	2330
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixGenPhotoHistos(PIX *pixs,

```
....
2330.          snprintf(buf, sizeof(buf),
"/tmp/lept/comp/tiledhistos.%d.pdf",
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2490
Status New

The pixDecideIfPhotoImage method calls the snprintf function, at line 2498 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	2559	2559
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixDecideIfPhotoImage(PIX *pix,

```
....
2559.              snprintf(buf, sizeof(buf),
"/tmp/lept/compplot/plot.%d", i);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2491
Status New

The compareTilesByHisto method calls the snprintf function, at line 2706 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	2777	2777
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method compareTilesByHisto(NUMAA *naa1,

```
....
2777.              snprintf(buf1, sizeof(buf1),
"/tmp/lept/comptile/plot.%d", i);
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2492
Status New

The compareTilesByHisto method calls the snprintf function, at line 2706 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	2788	2788
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method compareTilesByHisto(NUMAA *naa1,

```
....
2788.              snprintf(buf1, sizeof(buf1),
"/tmp/lept/comptile/plot.%d.png", i);
```

Unchecked Return Value\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2493
Status New

The compareTilesByHisto method calls the snprintf function, at line 2706 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	2792	2792
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method compareTilesByHisto(NUMAA *naa1,

```
....
2792.              snprintf(buf2, sizeof(buf2),
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2494
Status New

The pixCompareTilesByHisto method calls the snprintf function, at line 3011 of mobile-ffmpeg/compare.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	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	3090	3090
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixCompareTilesByHisto(PIX *pix1,

```
....
3090.              snprintf(buf, sizeof(buf), "%5.3f", score);
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2495
Status New

The pixMosaicColorShiftRGB method calls the snprintf function, at line 1834 of mobile-ffmpeg/enhance.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	mobile-ffmpeg/enhance.c	mobile-ffmpeg/enhance.c
Line	1870	1870
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/enhance.c
Method pixMosaicColorShiftRGB(PIX *pixs,

```
....
1870.          snprintf(buf, sizeof(buf), "%4.2f, %4.2f, %4.2f",
```

Unchecked Return Value\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2496
Status New

The pixMosaicColorShiftRGB method calls the snprintf function, at line 1834 of mobile-ffmpeg/enhance.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	mobile-ffmpeg/enhance.c	mobile-ffmpeg/enhance.c
Line	1879	1879
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/enhance.c
Method pixMosaicColorShiftRGB(PIX *pixs,

```
....
1879.          snprintf(buf, sizeof(buf), "%4.2f, %4.2f, %4.2f",
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2497
Status New

The pixMosaicColorShiftRGB method calls the snprintf function, at line 1834 of mobile-ffmpeg/enhance.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	mobile-ffmpeg/enhance.c	mobile-ffmpeg/enhance.c
Line	1888	1888
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/enhance.c
Method pixMosaicColorShiftRGB(PIX *pixs,

```
....
1888.          snprintf(buf, sizeof(buf), "%4.2f, %4.2f, %4.2f",
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2498
Status New

The format_combo_test method calls the snprintf function, at line 81 of mobile-ffmpeg/format_check_test.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	mobile-ffmpeg/format_check_test.c	mobile-ffmpeg/format_check_test.c
Line	117	117
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/format_check_test.c
Method format_combo_test (void)

```
....
117.                    snprintf (filename, sizeof (filename), "format-
check.%s", major_fmt_info.extension) ;
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2499
Status New

The format_combo_test method calls the snprintf function, at line 81 of mobile-ffmpeg/format_check_test.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	mobile-ffmpeg/format_check_test.c	mobile-ffmpeg/format_check_test.c
Line	125	125
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/format_check_test.c
Method format_combo_test (void)

```
....
125.                    {     snprintf (filename, sizeof (filename),
"._format-check.%s", major_fmt_info.extension) ;
```

Unchecked Return Value\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2500
Status New

The *format_filesize_string method calls the snprintf function, at line 93 of mobile-ffmpeg/frontend.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	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	100	100
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *format_filesize_string(char *string, int string_size, int filesize)

```
....
100.          snprintf(string, string_size, "%d bytes", filesize);
```

Unchecked Return Value\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2501
Status New

The *format_filesize_string method calls the snprintf function, at line 93 of mobile-ffmpeg/frontend.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	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	102	102
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *format_filesize_string(char *string, int string_size, int filesize)

```
....
102.          snprintf(string, string_size, "%2.2f KB", (float) filesize
/ CONST_KB);
```

Unchecked Return Value\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2502
Status New

The *format_filesize_string method calls the snprintf function, at line 93 of mobile-ffmpeg/frontend.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	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	104	104
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *format_filesize_string(char *string, int string_size, int filesize)

```
....
104.          snprintf(string, string_size, "%2.2f MB", (float) filesize
/ CONST_MB);
```

Unchecked Return Value\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2503
Status New

The *format_filesize_string method calls the snprintf function, at line 93 of mobile-ffmpeg/frontend.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	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	106	106
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *format_filesize_string(char *string, int string_size, int filesize)

```
....
106.          snprintf(string, string_size, "%2.2f GB", (float) filesize
/ CONST_GB);
```

Unchecked Return Value\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2504
Status New

The *format_duration_string method calls the snprintf function, at line 649 of mobile-ffmpeg/frontend.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	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	655	655
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *format_duration_string(SF_INFO * sfinfo, char *string, int string_size)

```
....
655.          snprintf(string, string_size, "Unknown");
```

Unchecked Return Value\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2505
Status New

The *format_duration_string method calls the snprintf function, at line 649 of mobile-ffmpeg/frontend.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	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	664	664
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static char *format_duration_string(SF_INFO * sfinfo, char *string, int string_size)

```
....
664.          snprintf(string, string_size, "%imin %1.1fsec", minutes,
seconds);
```

Unchecked Return Value\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2506
Status New

The main method calls the remove function, at line 1678 of mobile-ffmpeg/makepng.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	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1937	1937
Object	remove	remove

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1937.           remove(file_name);
```

Unchecked Return Value\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2507
Status New

The pixGetColorNearMaskBoundary method calls the snprintf function, at line 1346 of mobile-ffmpeg/pix3.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	mobile-ffmpeg/pix3.c	mobile-ffmpeg/pix3.c
Line	1383	1383
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pix3.c
Method pixGetColorNearMaskBoundary(PIX *pixs,

```
....
1383.          snprintf(op, sizeof(op), "d%d.%d", 2 * dist, 2 * dist);
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2508
Status New

The pixSplitDistributionFgBg method calls the snprintf function, at line 3372 of mobile-ffmpeg/pix4.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	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	3425	3425
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixSplitDistributionFgBg(PIX *pixs,

```
....
3425.          snprintf(buf, sizeof(buf), "score fract = %3.1f",
scorefract);
```

Unchecked Return Value\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2509
Status New

The pixDisplayColorArray method calls the snprintf function, at line 2759 of mobile-ffmpeg/pix4.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	mobile-ffmpeg/pix4.c	mobile-ffmpeg/pix4.c
Line	2785	2785
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pix4.c
Method pixDisplayColorArray(l_uint32 *carray,

```
....
2785.              snprintf(textstr, sizeof(textstr),
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2510
Status New

The pixaReadBoth method calls the snprintf function, at line 2873 of mobile-ffmpeg/pixabasic.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	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2888	2888
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaReadBoth(const char *filename)

```
....
2888.      snprintf(buf, sizeof(buf), "%s", sname);
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2511
Status New

The pixaDisplayOnLattice method calls the snprintf function, at line 530 of mobile-ffmpeg/pixafunc2.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	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	610	610
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaDisplayOnLattice(PIXA *pixa,

```
....
610.      snprintf(buf, sizeof(buf), "n = %d", boxaGetCount(boxa));
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2512
Status New

The pixaDisplayTiledWithText method calls the snprintf function, at line 1292 of mobile-ffmpeg/pixafunc2.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	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	1342	1342
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaDisplayTiledWithText(PIXA *pixa,

```
....
1342.             snprintf(buf, sizeof(buf), "%s", textstr);
```

Unchecked Return Value\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2513
Status New

The pixaDisplayTiledByIndex method calls the snprintf function, at line 1391 of mobile-ffmpeg/pixafunc2.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	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	1447	1447
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaDisplayTiledByIndex(PIXA *pixa,

```
....
1447.              snprintf(buf, sizeof(buf), "%s", textstr);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2514
Status	New

The pixaMakeFromTiledPixa method calls the snprintf function, at line 2099 of mobile-ffmpeg/pixafunc2.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	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	2131	2131
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaMakeFromTiledPixa(PIXA *pixas,

```
....
2131.          snprintf(buf, sizeof(buf), "%d", i);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2515
Status	New

The pixaSplitIntoFiles method calls the snprintf function, at line 2381 of mobile-ffmpeg/pixafunc2.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	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	2417	2417
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaSplitIntoFiles(PIXA *pixas,

```
....
2417.              snprintf(buf, sizeof(buf),
"/tmp/lept/split/split%d.pa", i + 1);
```

Unchecked Return Value\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2516
Status New

The pixaSplitIntoFiles method calls the snprintf function, at line 2381 of mobile-ffmpeg/pixafunc2.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	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	2421	2421
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaSplitIntoFiles(PIXA *pixas,

```
....
2421.              snprintf(buf, sizeof(buf),
"/tmp/lept/split/split%d.tif", i + 1);
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2517
Status New

The pixaSplitIntoFiles method calls the snprintf function, at line 2381 of mobile-ffmpeg/pixafunc2.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	mobile-ffmpeg/pixafunc2.c	mobile-ffmpeg/pixafunc2.c
Line	2427	2427
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/pixafunc2.c
Method pixaSplitIntoFiles(PIXA *pixas,

```
....
2427.              snprintf(buf, sizeof(buf),
"/tmp/lept/split/split%d.pdf", i + 1);
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2518
Status New

The main method calls the snprintf function, at line 46 of mobile-ffmpeg/recog_bootnum3.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	mobile-ffmpeg/recog_bootnum3.c	mobile-ffmpeg/recog_bootnum3.c
Line	67	67
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/recog_bootnum3.c
Method l_int32 main(int argc,

```
....
67.          snprintf(buf, sizeof(buf), "recog/digits/digit%d.comp.tif",
i);
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2519
Status New

The res0_free_look method calls the sprintf function, at line 73 of mobile-ffmpeg/res0.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	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	91	91
Object	sprintf	sprintf

Code Snippet
File Name mobile-ffmpeg/res0.c
Method void res0_free_look(vorbis_look_residue *i){

```
....
91.             sprintf(buffer,"res_sub%d_part%d_pass%d.vqd",look-
>submap,j,k);
```

Unchecked Return Value\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2520
Status New

The **_01class method calls the sprintf function, at line 406 of mobile-ffmpeg/res0.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	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	456	456
Object	sprintf	sprintf

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static long **_01class(vorbis_block *vb,vorbis_look_residue *vl,

```
....
456.        sprintf(buffer,"resaux_%d.vqd",look->train_seq);
```

Unchecked Return Value\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2521
Status New

The **_2class method calls the sprintf function, at line 473 of mobile-ffmpeg/res0.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	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	515	515
Object	sprintf	sprintf

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static long **_2class(vorbis_block *vb,vorbis_look_residue *vl,int **in,

```
....
515.    sprintf(buffer,"resaux_%d.vqd",look->train_seq);
```

Unchecked Return Value\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2522
Status New

The oc_state_dump_frame method calls the sprintf function, at line 1068 of mobile-ffmpeg/state.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	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	1096	1096
Object	sprintf	sprintf

Code Snippet
File Name mobile-ffmpeg/state.c
Method int oc_state_dump_frame(const oc_theora_state *_state,int _frame,

```
....
1096.    sprintf(fname,"%08i%s.png",(int)(iframe+pframe),_suf);
```

Unchecked Return Value\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2523
Status New

The t2p_write_pdf_name method calls the snprintf function, at line 3889 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	3904	3904
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_name(unsigned char* name, TIFF* output){

```
....
3904.                    snprintf(buffer, sizeof(buffer), "#%.2X",
name[i]);
```

Unchecked Return Value\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2524
Status New

The t2p_write_pdf_name method calls the snprintf function, at line 3889 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	3910	3910
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_name(unsigned char* name, TIFF* output){

```
....
3910.                    snprintf(buffer, sizeof(buffer), "#%.2X",
name[i]);
```

Unchecked Return Value\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2525
Status New

The t2p_write_pdf_name method calls the snprintf function, at line 3889 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	3918	3918
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_name(unsigned char* name, TIFF* output){

```
....
3918.                                   snprintf(buffer, sizeof(buffer),
"#%.2X", name[i]);
```

Unchecked Return Value\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2526
Status New

The t2p_write_pdf_name method calls the snprintf function, at line 3889 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	3923	3923
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_name(unsigned char* name, TIFF* output){

```
....
3923.                                   snprintf(buffer, sizeof(buffer),
"#%.2X", name[i]);
```

Unchecked Return Value\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2527
Status New

The t2p_write_pdf_name method calls the snprintf function, at line 3889 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	3928	3928
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_name(unsigned char* name, TIFF* output){

```
....
3928.                                   snprintf(buffer, sizeof(buffer),
"#%.2X", name[i]);
```

Unchecked Return Value\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2528
Status New

The t2p_write_pdf_name method calls the snprintf function, at line 3889 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	3933	3933
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_name(unsigned char* name, TIFF* output){

```
....
3933.                                   snprintf(buffer, sizeof(buffer),
"#%.2X", name[i]);
```

Unchecked Return Value\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2529
Status New

The t2p_write_pdf_name method calls the snprintf function, at line 3889 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	3938	3938
Object	snprintf	snprintf

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_name(unsigned char* name, TIFF* output){

```
....
3938.                                   snprintf(buffer, sizeof(buffer),
"#%.2X", name[i]);
```

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=1060095&projectid=60085&pathid=2160
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by data at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	609	616
Object	null	data

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
609.         return NULL;
....
616.     return((char *)oy->data+oy->fill);
```

NULL Pointer Dereference\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2161
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by data at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	588	616
Object	null	data

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
588.    if(ogg_sync_check(oy)) return NULL;
....
616.    return((char *)oy->data+oy->fill);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2162
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by returned at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	588	591
Object	null	returned

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
588.    if(ogg_sync_check(oy)) return NULL;
....
591.    if(oy->returned){
```

NULL Pointer Dereference\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2163
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by returned at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	609	591
Object	null	returned

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
609.         return NULL;
....
591.     if(oy->returned){
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2164
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by fill at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	588	616
Object	null	fill

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
588.     if(ogg_sync_check(oy)) return NULL;
....
616.     return((char *)oy->data+oy->fill);
```

NULL Pointer Dereference\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2165
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by fill at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	609	616
Object	null	fill

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
609.         return NULL;
....
616.     return((char *)oy->data+oy->fill);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2166
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by fill at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	588	592
Object	null	fill

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
588.     if(ogg_sync_check(oy)) return NULL;
....
592.       oy->fill-=oy->returned;
```

NULL Pointer Dereference\Path 8:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2167
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by fill at mobile-ffmpeg/framing.c in line 587.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	609	592
Object	null	fill

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
609.         return NULL;
....
592.       oy->fill-=oy->returned;
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2168
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by fill at mobile-ffmpeg/framing.c in line 619.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	588	622
Object	null	fill

Code Snippet
File Name mobile-ffmpeg/framing.c
Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
588.     if(ogg_sync_check(oy)) return NULL;
```

File Name mobile-ffmpeg/framing.c
Method int ogg_sync_wrote(ogg_sync_state *oy, long bytes){

```
....
622.    oy->fill+=bytes;
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2169
Status	New

The variable declared in null at mobile-ffmpeg/framing.c in line 587 is not initialized when it is used by fill at mobile-ffmpeg/framing.c in line 619.

	Source	Destination
File	mobile-ffmpeg/framing.c	mobile-ffmpeg/framing.c
Line	609	622
Object	null	fill

Code Snippet

File Name mobile-ffmpeg/framing.c

Method char *ogg_sync_buffer(ogg_sync_state *oy, long size){

```
....
609.        return NULL;
```

File Name mobile-ffmpeg/framing.c

Method int ogg_sync_wrote(ogg_sync_state *oy, long bytes){

```
....
622.    oy->fill+=bytes;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2170
Status	New

The variable declared in null at mobile-ffmpeg/kvazaar.c in line 305 is not initialized when it is used by ref_list at mobile-ffmpeg/kvazaar.c in line 145.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	352	152

Object	null	ref_list

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static int kvazaar_field_encoding_adapter(kvz_encoder *enc,

```
....
352.    if (!kvazaar_encode(enc, second_field, &second.data_out,
&second.len_out, NULL, NULL, NULL)) {
```

File Name mobile-ffmpeg/kvazaar.c

Method static void set_frame_info(kvz_frame_info *const info, const encoder_state_t *const state)

```
....
152.    memset(info->ref_list[0], 0, 16 * sizeof(int));
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2171
Status	New

The variable declared in null at mobile-ffmpeg/kvazaar.c in line 305 is not initialized when it is used by ref_list at mobile-ffmpeg/kvazaar.c in line 145.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	352	153
Object	null	ref_list

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static int kvazaar_field_encoding_adapter(kvz_encoder *enc,

```
....
352.    if (!kvazaar_encode(enc, second_field, &second.data_out,
&second.len_out, NULL, NULL, NULL)) {
```

File Name mobile-ffmpeg/kvazaar.c

Method static void set_frame_info(kvz_frame_info *const info, const encoder_state_t *const state)

```
....
153.    memset(info->ref_list[1], 0, 16 * sizeof(int));
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2172
Status	New

The variable declared in null at mobile-ffmpeg/makepng.c in line 1365 is not initialized when it is used by endptr at mobile-ffmpeg/makepng.c in line 1365.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1367	1370
Object	null	endptr

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method bval(png_const_structrp png_ptr, png_charp param, unsigned int maxval)

```
....
1367.     char *endptr = NULL;
....
1370.     if (param[0] && *endptr == 0 && l <= maxval)
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2173
Status	New

The variable declared in null at mobile-ffmpeg/SDL_wave.c in line 448 is not initialized when it is used by index at mobile-ffmpeg/SDL_wave.c in line 338.

	Source	Destination
File	mobile-ffmpeg/SDL_wave.c	mobile-ffmpeg/SDL_wave.c
Line	612	377
Object	null	index

Code Snippet
File Name mobile-ffmpeg/SDL_wave.c
Method SDL_LoadWAV_RW(SDL_RWops * src, int freesrc,

```
....
612.      *audio_buf = NULL;
```

File Name mobile-ffmpeg/SDL_wave.c

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

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

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2174
Status	New

The variable declared in null at mobile-ffmpeg/SDL_wave.c in line 448 is not initialized when it is used by index at mobile-ffmpeg/SDL_wave.c in line 338.

	Source	Destination
File	mobile-ffmpeg/SDL_wave.c	mobile-ffmpeg/SDL_wave.c
Line	615	377
Object	null	index

Code Snippet

File Name mobile-ffmpeg/SDL_wave.c

Method SDL_LoadWAV_RW(SDL_RWops * src, int freesrc,

```
....
615.          *audio_buf = NULL;
```

File Name mobile-ffmpeg/SDL_wave.c

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

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

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2175
Status	New

The variable declared in null at mobile-ffmpeg/SDL_wave.c in line 448 is not initialized when it is used by hPredictor at mobile-ffmpeg/SDL_wave.c in line 119.

	Source	Destination
File	mobile-ffmpeg/SDL_wave.c	mobile-ffmpeg/SDL_wave.c
Line	612	150
Object	null	hPredictor

Code Snippet
File Name mobile-ffmpeg/SDL_wave.c
Method SDL_LoadWAV_RW(SDL_RWops * src, int freesrc,

```
....
612.      *audio_buf = NULL;
```

File Name mobile-ffmpeg/SDL_wave.c
Method MS_ADPCM_decode(Uint8 ** audio_buf, Uint32 * audio_len)

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

NULL Pointer Dereference\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2176
Status New

The variable declared in null at mobile-ffmpeg/SDL_wave.c in line 448 is not initialized when it is used by hPredictor at mobile-ffmpeg/SDL_wave.c in line 119.

	Source	Destination
File	mobile-ffmpeg/SDL_wave.c	mobile-ffmpeg/SDL_wave.c
Line	615	150
Object	null	hPredictor

Code Snippet
File Name mobile-ffmpeg/SDL_wave.c
Method SDL_LoadWAV_RW(SDL_RWops * src, int freesrc,

```
....
615.          *audio_buf = NULL;
```

File Name mobile-ffmpeg/SDL_wave.c

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

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

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2177
Status	New

The variable declared in null at mobile-ffmpeg/SDL_wave.c in line 448 is not initialized when it is used by hPredictor at mobile-ffmpeg/SDL_wave.c in line 119.

	Source	Destination
File	mobile-ffmpeg/SDL_wave.c	mobile-ffmpeg/SDL_wave.c
Line	615	148
Object	null	hPredictor

Code Snippet

File Name mobile-ffmpeg/SDL_wave.c

Method SDL_LoadWAV_RW(SDL_RWops * src, int freesrc,

```
....
615.          *audio_buf = NULL;
```

File Name mobile-ffmpeg/SDL_wave.c

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

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

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2178
Status	New

The variable declared in null at mobile-ffmpeg/SDL_wave.c in line 448 is not initialized when it is used by hPredictor at mobile-ffmpeg/SDL_wave.c in line 119.

	Source	Destination
File	mobile-ffmpeg/SDL_wave.c	mobile-ffmpeg/SDL_wave.c

Line	612	148
Object	null	hPredictor

Code Snippet
File Name mobile-ffmpeg/SDL_wave.c
Method SDL_LoadWAV_RW(SDL_RWops * src, int freesrc,

```
....
612.      *audio_buf = NULL;
```

File Name mobile-ffmpeg/SDL_wave.c
Method MS_ADPCM_decode(Uint8 ** audio_buf, Uint32 * audio_len)

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

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2179
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by doblend at mobile-ffmpeg/ttgxvar.c in line 2777.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	2811
Object	null	doblend

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.      FT_MM_Var*           mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Blend(TT_Face face,

```
....
2811.      if ( face->doblend )
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2180
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by face at mobile-ffmpeg/ttgxvar.c in line 1185.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	1204
Object	null	face

Code Snippet

File Name mobile-ffmpeg/ttgxvar.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.      FT_MM_Var*           mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c

Method ft_var_load_mvar(TT_Face face)

```
....
1204.      error = face->goto_table( face, TTAG_MVAR, stream, &table_len
);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2181
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by is_cff2 at mobile-ffmpeg/ttgxvar.c in line 2505.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	2565
Object	null	is_cff2

Code Snippet

File Name mobile-ffmpeg/ttgxvar.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c

Method tt_set_mm_blend(TT_Face face,

```
....
2565.       if ( !face->is_cff2 && !blend->glyphoffsets )
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2182
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by face at mobile-ffmpeg/ttgxvar.c in line 333.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	351
Object	null	face

Code Snippet

File Name mobile-ffmpeg/ttgxvar.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c

Method ft_var_load_avar(TT_Face face)

```
....
351.        error = face->goto_table( face, TTAG_avar, stream, &table_len
);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2183

Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by blend at mobile-ffmpeg/ttgxvar.c in line 2505.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	2530
Object	null	blend

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name mobile-ffmpeg/ttgxvar.c
Method tt_set_mm_blend(TT_Face face,

```
....
2530.       if ( !face->blend )
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2184
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by blend at mobile-ffmpeg/ttgxvar.c in line 2858.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	2952
Object	null	blend

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name	mobile-ffmpeg/ttgxvar.c
Method	TT_Set_Var_Design(TT_Face face,

```
....
2952.       if ( !face->blend->avar_loaded )
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2185
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by doblend at mobile-ffmpeg/ttgxvar.c in line 3000.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2045	3034
Object	null	doblend

Code Snippet

File Name	mobile-ffmpeg/ttgxvar.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name	mobile-ffmpeg/ttgxvar.c
Method	TT_Get_Var_Design(TT_Face face,

```
....
3034.       if ( face->doblend )
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2186
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 3752 is not initialized when it is used by x at mobile-ffmpeg/ttgxvar.c in line 3526.

	Source	Destination

File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	3763	3544
Object	null	x

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name mobile-ffmpeg/ttgxvar.c
Method tt_delta_shift(int p1,

```
....
3544.        out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2187
Status New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 3752 is not initialized when it is used by x at mobile-ffmpeg/ttgxvar.c in line 3526.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	3763	3550
Object	null	x

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name mobile-ffmpeg/ttgxvar.c
Method tt_delta_shift(int p1,

```
....
3550.         out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2188
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 3752 is not initialized when it is used by y at mobile-ffmpeg/ttgxvar.c in line 3526.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	3763	3551
Object	null	y

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name mobile-ffmpeg/ttgxvar.c
Method tt_delta_shift(int p1,

```
....
3551.         out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2189
Status	New

The variable declared in null at mobile-ffmpeg/ttgxvar.c in line 3752 is not initialized when it is used by y at mobile-ffmpeg/ttgxvar.c in line 3526.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	3763	3545

Object	null	y

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name mobile-ffmpeg/ttgxvar.c
Method tt_delta_shift(int p1,

```
....
3545.        out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2190
Status	New

The variable declared in 0 at mobile-ffmpeg/bitwise.c in line 179 is not initialized when it is used by Pointer at mobile-ffmpeg/bitwise.c in line 179.

	Source	Destination
File	mobile-ffmpeg/bitwise.c	mobile-ffmpeg/bitwise.c
Line	215	215
Object	0	Pointer

Code Snippet
File Name mobile-ffmpeg/bitwise.c
Method static void oggpack_writecopy_helper(oggpack_buffer *b,

```
....
215.      *b->ptr=0;
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2191
Status	New

The variable declared in 0 at mobile-ffmpeg/DecUT_DecExt.cpp in line 517 is not initialized when it is used by m_pDec at mobile-ffmpeg/DecUT_DecExt.cpp in line 517.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	596	600
Object	0	m_pDec

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestGetDecStatistics() {

```
....
596.    iError = 0;
....
600.    m_pDec->GetOption (DECODER_OPTION_GET_STATISTICS, &sDecStatic);
```

NULL Pointer Dereference\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2192
Status New

The variable declared in 0 at mobile-ffmpeg/ttgxvar.c in line 2036 is not initialized when it is used by num_designs at mobile-ffmpeg/ttgxvar.c in line 2036.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	2205	2204
Object	0	num_designs

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2205.          ~0U;                   /* meaningless in this context;
each glyph */
....
2204.        mmvar->num_designs =
```

NULL Pointer Dereference\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2193
Status New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by frames_done at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	103
Object	encoder	frames_done

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
103.    encoder->frames_done = 0;
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2194
Status New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by frames_started at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	102
Object	encoder	frames_started

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
102.    encoder->frames_started = 0;
```

NULL Pointer Dereference\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2195
Status New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by states at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	112
Object	encoder	states

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
112.    encoder->states = calloc(encoder->num_encoder_states,
sizeof(encoder_state_t));
```

NULL Pointer Dereference\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2196
Status New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by previous_encoder_state at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	130
Object	encoder	previous_encoder_state

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
130.        encoder->states[i].previous_encoder_state = &encoder-
>states[(i - 1) % encoder->num_encoder_states];
```

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=2197
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by QP at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	123
Object	encoder	QP

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
123.        encoder->states[i].frame->QP = (int8_t)cfg->qp;
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2198
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by encoder_control at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	118
Object	encoder	encoder_control

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
118.        encoder->states[i].encoder_control = encoder->control;
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=2199
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by out_state_num at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	101
Object	encoder	out_state_num

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
101.    encoder->out_state_num = 0;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2200
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by cur_state_num at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	100
Object	encoder	cur_state_num

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
100.    encoder->cur_state_num = 0;
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=2201
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by num_encoder_states at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	99
Object	encoder	num_encoder_states

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
99.     encoder->num_encoder_states = encoder->control->cfg.owf + 1;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2202
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by num at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	135
Object	encoder	num

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
135.     encoder->states[encoder->cur_state_num].frame->num = -1;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=600

	85&pathid=2203
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by previous_encoder_state at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	128
Object	encoder	previous_encoder_state

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
128.        encoder->states[i].previous_encoder_state = &encoder-
>states[encoder->num_encoder_states - 1];
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2204
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by control at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	94
Object	encoder	control

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
94.    encoder->control = kvz_encoder_control_init(cfg);
```

NULL Pointer Dereference\Path 46:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2205
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by control at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	118
Object	encoder	control

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
118.      encoder->states[i].encoder_control = encoder->control;
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2206
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by control at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	106
Object	encoder	control

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
106.     if(!kvz_get_rc_data(encoder->control)) {
```

NULL Pointer Dereference\Path 48:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2207
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by control at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	95
Object	encoder	control

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
95.     if (!encoder->control) {
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2208
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by control at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	99
Object	encoder	control

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.     kvz_encoder *encoder = NULL;
....
99.     encoder->num_encoder_states = encoder->control->cfg.owf + 1;
```

NULL Pointer Dereference\Path 50:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2209
Status	New

The variable declared in encoder at mobile-ffmpeg/kvazaar.c in line 78 is not initialized when it is used by input_buffer at mobile-ffmpeg/kvazaar.c in line 78.

	Source	Destination
File	mobile-ffmpeg/kvazaar.c	mobile-ffmpeg/kvazaar.c
Line	80	110
Object	encoder	input_buffer

Code Snippet
File Name mobile-ffmpeg/kvazaar.c
Method static kvz_encoder * kvazaar_open(const kvz_config *cfg)

```
....
80.    kvz_encoder *encoder = NULL;
....
110.    kvz_init_input_frame_buffer(&encoder->input_buffer);
```

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=1060095&projectid=60085&pathid=2428
Status	New

Method random_number at line 320 of mobile-ffmpeg/abx.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	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	327	327
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int random_number (void)

```
....
327.      val  = t.tv_sec ^ t.tv_usec ^ rand();
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2429
Status	New

Method change_direction at line 376 of mobile-ffmpeg/ath.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	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	414	414
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int change_direction (amplitude_t* const a, direction_t new_direction)

```
....
414.      a->direction_change = 1 + rand () * (a->sample_freq *
DELAY_UNTIL_XCHG / RAND_MAX);
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2430
Status	New

Method gaussDistribSampling at line 2551 of mobile-ffmpeg/convolve.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	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	2559	2559
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method gaussDistribSampling()

```
....
2559.               frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2431
Status	New

Method gaussDistribSampling at line 2551 of mobile-ffmpeg/convolve.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	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	2561	2561
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method gaussDistribSampling()

```
....
2561.               frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2432
Status	New

Method DecoderInterfaceTest::Init at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	90	90
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::Init() {

```
....
90.    m_sDecParam.uiCpuLoad = rand() % 100;
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2433
Status	New

Method DecoderInterfaceTest::Init at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	91	91
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::Init() {

```
....
91.    m_sDecParam.uiTargetDqLayer = rand() % 100;
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2434
Status	New

Method DecoderInterfaceTest::Init at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	92	92
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::Init() {

```
....
92.    m_sDecParam.eEcActiveIdc = (ERROR_CON_IDC) (rand() & 7);
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2435
Status	New

Method DecoderInterfaceTest::Init at line 85 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	94	94
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::Init() {

```
....
94.    m_sDecParam.sVideoProperty.eVideoBsType = (VIDEO_BITSTREAM_TYPE)
(rand() % 2);
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2436
Status	New

Method DecoderInterfaceTest::ValidInit at line 105 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	111	111
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method int32_t DecoderInterfaceTest::ValidInit() {

```
....
111.    m_sDecParam.eEcActiveIdc = (ERROR_CON_IDC) (rand() & 7);
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2437
Status	New

Method DecoderInterfaceTest::MockPacketType at line 189 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	220	220
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::MockPacketType (const EWelsNalUnitType eNalUnitType, const int iPacketLength) {

```
....
220.      m_szBuffer[m_iBufLength++] = rand() % 256;
```

Use of Insufficiently Random Values\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2438
Status	New

Method DecoderInterfaceTest::TestParseOnlyAPI at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	278	278
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
278.      m_sDecParam.uiCpuLoad = rand() % 100;
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2439
Status	New

Method DecoderInterfaceTest::TestParseOnlyAPI at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	283	283
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
283.      m_sDecParam.sVideoProperty.eVideoBsType =
(VIDEO_BITSTREAM_TYPE) (rand() % 2);
```

Use of Insufficiently Random Values\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2440
Status	New

Method DecoderInterfaceTest::TestParseOnlyAPI at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	311	311
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
311.      m_sDecParam.uiCpuLoad = rand() % 100;
```

Use of Insufficiently Random Values\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2441
Status	New

Method DecoderInterfaceTest::TestParseOnlyAPI at line 260 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	316	316
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestParseOnlyAPI() {

```
....
316.      m_sDecParam.sVideoProperty.eVideoBsType =
(VIDEO_BITSTREAM_TYPE) (rand() % 2);
```

Use of Insufficiently Random Values\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2442
Status	New

Method DecoderInterfaceTest::TestEndOfStream at line 341 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	355	355
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestEndOfStream() {

```
....
355.      iTmp = rand();
```

Use of Insufficiently Random Values\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2443
Status	New

Method DecoderInterfaceTest::TestVclNal at line 405 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	415	415
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestVclNal() {

```
....
415.    iTmp = rand();
```

Use of Insufficiently Random Values\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2444
Status	New

Method DecoderInterfaceTest::TestErrorConIdc at line 469 of mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	488	488
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestErrorConIdc() {

```
....
488.    iTmp = rand() & 7;
```

Use of Insufficiently Random Values\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2445
Status	New

Method DecoderParseSyntaxTest::Init at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp 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	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	182	182
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
182.    m_sDecParam.uiCpuLoad = rand() % 100;
```

Use of Insufficiently Random Values\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2446
Status	New

Method DecoderParseSyntaxTest::Init at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp 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	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	183	183
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
183.    m_sDecParam.uiTargetDqLayer = rand() % 100;
```

Use of Insufficiently Random Values\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2447
Status	New

Method DecoderParseSyntaxTest::Init at line 172 of mobile-ffmpeg/DecUT_ParseSyntax.cpp 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	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	186	186
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method int32_t DecoderParseSyntaxTest::Init() {

```
....
186.    m_sDecParam.sVideoProperty.eVideoBsType = (VIDEO_BITSTREAM_TYPE)
(rand() % 2);
```

Use of Insufficiently Random Values\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2448
Status	New

Method TEST at line 528 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	529	529
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI16x16LumaPredDcTop) {

```
....
529.    const int32_t kiStride = rand() % 16 + 16;
```

Use of Insufficiently Random Values\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2449
Status	New

Method TEST at line 528 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	536	536
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI16x16LumaPredDcTop) {

```
....
536.      pRef[i] = rand() % 256 + 1;
```

Use of Insufficiently Random Values\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2450
Status	New

Method TEST at line 10 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	14	14
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredV) {

```
....
14.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2451
Status	New

Method TEST at line 26 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	27	27
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredH) {

```
....
27.    const int32_t kiStride = rand() % 256 + 16;
```

Use of Insufficiently Random Values\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2452
Status	New

Method TEST at line 26 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	35	35
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredH) {

```
....
35.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2453
Status	New

Method TEST at line 65 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	71	71
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredDDL) {

```
....
71.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2454
Status	New

Method TEST at line 106 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	112	112
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredDDLTop) {

```
....
112.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2455
Status	New

Method TEST at line 138 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	139	139
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredDDR) {

```
....
139.    const int32_t kiStride = rand() % 256 + 16;
```

Use of Insufficiently Random Values\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2456
Status	New

Method TEST at line 138 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	147	147
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredDDR) {

```
....
147.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2457
Status	New

Method TEST at line 195 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	201	201
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredVL) {

```
....
201.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2458
Status	New

Method TEST at line 241 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	247	247
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredVLTop) {

```
....
247.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2459
Status	New

Method TEST at line 286 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	287	287
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredVR) {

```
....
287.    const int32_t kiStride = rand() % 256 + 16;
```

Use of Insufficiently Random Values\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2460
Status	New

Method TEST at line 286 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	294	294
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredVR) {

```
....
294.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2461
Status	New

Method TEST at line 339 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	340	340
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredHU) {

```
....
340.    const int32_t kiStride = rand() % 256 + 16;
```

Use of Insufficiently Random Values\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2462
Status	New

Method TEST at line 339 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	348	348
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredHU) {

```
....
348.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2463
Status	New

Method TEST at line 385 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	386	386
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredHD) {

```
....
386.    const int32_t kiStride = rand() % 256 + 16;
```

Use of Insufficiently Random Values\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2464
Status	New

Method TEST at line 385 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	394	394
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI4x4LumaPredHD) {

```
....
394.      pRef[i] = rand() % 256;
```

Use of Insufficiently Random Values\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2465
Status	New

Method TEST at line 439 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	443	443
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetIChromaPredV) {

```
....
443.      pRef[i] = rand() % 256 + 1;
```

Use of Insufficiently Random Values\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2466
Status	New

Method TEST at line 455 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	456	456
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI16x16LumaPredPlane) {

```
....
456.    const int32_t kiStride = rand() % 16 + 16;
```

Use of Insufficiently Random Values\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2467
Status	New

Method TEST at line 455 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	463	463
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI16x16LumaPredPlane) {

```
....
463.      pRef[i] = rand() % 256 + 1;
```

Use of Insufficiently Random Values\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2468
Status	New

Method TEST at line 495 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	496	496
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI16x16LumaPredDc) {

```
....
496.    const int32_t kiStride = rand() % 16 + 16;
```

Use of Insufficiently Random Values\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2469
Status	New

Method TEST at line 495 of mobile-ffmpeg/EncUT_GetIntraPredictor.cpp 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	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp	mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Line	503	503
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/EncUT_GetIntraPredictor.cpp
Method TEST (GetIntraPredictorTest, TestGetI16x16LumaPredDc) {

```
....
503.      pRef[i] = rand() % 256 + 1;
```

Use of Insufficiently Random Values\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2470
Status	New

Method pixGetRandomPixel at line 413 of mobile-ffmpeg/pix2.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	mobile-ffmpeg/pix2.c	mobile-ffmpeg/pix2.c
Line	433	433
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/pix2.c
Method pixGetRandomPixel(PIX *pix,

```
....
433.        x = rand() % w;
```

Use of Insufficiently Random Values\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2471
Status	New

Method pixGetRandomPixel at line 413 of mobile-ffmpeg/pix2.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	mobile-ffmpeg/pix2.c	mobile-ffmpeg/pix2.c
Line	434	434
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/pix2.c
Method pixGetRandomPixel(PIX *pix,

```
....
434.        y = rand() % h;
```

Use of Insufficiently Random Values\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2472
Status	New

Method t2p_write_pdf_trailer at line 5402 of mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	5411	5411
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method tsize_t t2p_write_pdf_trailer(T2P* t2p, TIFF* output)

```
....
5411.             snprintf(t2p->pdf_fileid + i, 9, "%.8X", rand());
```

Use of Insufficiently Random Values\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2473
Status	New

Method main at line 609 of mobile-ffmpeg/transcoder_example.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	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	710	710
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
710.    ogg_stream_init(&vo,rand());
```

Use of Insufficiently Random Values\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2474
Status	New

Method main at line 609 of mobile-ffmpeg/transcoder_example.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	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	711	711
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
711.    ogg_stream_init(&to,rand()); /* oops, add one ot the above */
```

Use of Insufficiently Random Values\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2475
Status	New

Method generateRandomNumberArray at line 237 of mobile-ffmpeg/warper.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	mobile-ffmpeg/warper.c	mobile-ffmpeg/warper.c
Line	249	249
Object	rand	rand

Code Snippet
File Name mobile-ffmpeg/warper.c
Method generateRandomNumberArray(l_int32 size)

```
....
249.          randa[i] = 0.5 * (1.0 + (l_float64)rand() /
(l_float64)RAND_MAX);
```

Use of Insufficiently Random Values\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2476
Status	New

Method open_amplifier at line 306 of mobile-ffmpeg/ath.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	319	319
Object	srand	srand

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int open_amplifier (

```
....
319.      srand ( time (NULL) );
```

Use of Insufficiently Random Values\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2477
Status	New

Method main at line 609 of mobile-ffmpeg/transcoder_example.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	709	709
Object	srand	srand

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
709.    srand(time(NULL));
```

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=1060095&projectid=60085&pathid=840
Status	New

The buffer allocated by <= in mobile-ffmpeg/abx.c at line 337 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c

Line	349	349
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/abx.c
Method long double prob (int last, int total)

```
....
349.      for ( i = 0; i <= last; i++ ) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=841
Status	New

The buffer allocated by <= in mobile-ffmpeg/colorspace.c at line 702 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/colorspace.c	mobile-ffmpeg/colorspace.c
Line	738	738
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/colorspace.c
Method pixMakeRangeMaskHS(PIX *pixs,

```
....
738.          for (i = 0; i <= hend; i++)
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=842
Status	New

The buffer allocated by <= in mobile-ffmpeg/colorspace.c at line 801 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/colorspace.c	mobile-ffmpeg/colorspace.c
Line	837	837
Object	<=	<=

Code Snippet	
File Name	mobile-ffmpeg/colorspace.c
Method	pixMakeRangeMaskHV(PIX *pixs,

```
....
837.          for (i = 0; i <= hend; i++)
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=843
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 314 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	363	363
Object	<=	<=

Code Snippet	
File Name	mobile-ffmpeg/convolve.c
Method	blockconvLow(l_uint32 *data,

```
....
363.      for (i = 0; i <= hc; i++) {    /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=844
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 314 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	367	367
Object	<=	<=

Code Snippet	
File Name	mobile-ffmpeg/convolve.c

Method	blockconvLow(l_uint32 *data,

```
....
367.          for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=845
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 314 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	392	392
Object	<=	<=

Code Snippet	
File Name	mobile-ffmpeg/convolve.c
Method	blockconvLow(l_uint32 *data,

```
....
392.          for (j = 0; j <= wc; 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=1060095&projectid=60085&pathid=846
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 314 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	415	415
Object	<=	<=

Code Snippet	
File Name	mobile-ffmpeg/convolve.c
Method	blockconvLow(l_uint32 *data,

```
....
415.          for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=847
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	1670	1670
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method blocksumLow(l_uint32 *datad,

```
....
1670.      for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=848
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	1674	1674
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method blocksumLow(l_uint32 *datad,

```
....
1674.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=849
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	1699	1699
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method blocksumLow(l_uint32 *datad,

```
....
1699.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=850
Status	New

The buffer allocated by <= in mobile-ffmpeg/convolve.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/convolve.c	mobile-ffmpeg/convolve.c
Line	1722	1722
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/convolve.c
Method blocksumLow(l_uint32 *datad,

```
....
1722.          for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=851
Status	New

The buffer allocated by <= in mobile-ffmpeg/DecUT_DecExt.cpp at line 227 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	233	233
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestInitUninit() {

```
....
233.    for (int i = 0; i <= (int)
DECODER_OPTION_TRACE_CALLBACK_CONTEXT; ++i) {
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=852
Status	New

The buffer allocated by <= in mobile-ffmpeg/DecUT_DecExt.cpp at line 227 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	252	252
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::TestInitUninit() {

```
....
252.    for (int i = 0; i <= (int)
DECODER_OPTION_TRACE_CALLBACK_CONTEXT; ++i) {
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=853
Status	New

The buffer allocated by <= in mobile-ffmpeg/graphics.c at line 823 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/graphics.c	mobile-ffmpeg/graphics.c
Line	836	836
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/graphics.c
Method generatePtaFilledCircle(l_int32 radius)

```
....
836.      for (y = 0; y <= 2 * radius; y++) {
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=854
Status	New

The buffer allocated by <= in mobile-ffmpeg/graphics.c at line 823 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/graphics.c	mobile-ffmpeg/graphics.c
Line	837	837
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/graphics.c
Method generatePtaFilledCircle(l_int32 radius)

```
....
837.          for (x = 0; x <= 2 * radius; x++) {
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=855
Status	New

The buffer allocated by <= in mobile-ffmpeg/makepng.c at line 390 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	540	540
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
540.              for (x=0; x<=size_max; ++x)
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=856
Status	New

The buffer allocated by <= in mobile-ffmpeg/makepng.c at line 390 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	561	561
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
561.              for (x=0; x<=size_max; ++x)
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=857
Status	New

The buffer allocated by <= in mobile-ffmpeg/makepng.c at line 390 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	592	592
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
592.              for (x=0; x<=size_max; ++x)
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=858
Status	New

The buffer allocated by <= in mobile-ffmpeg/makepng.c at line 390 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	628	628
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
628.              for (x=0; x<=size_max; ++x)
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=859
Status	New

The buffer allocated by <= in mobile-ffmpeg/makepng.c at line 390 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	667	667
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
667.                  for (x=0; x<=size_max; ++x)
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=860
Status	New

The buffer allocated by <= in mobile-ffmpeg/makepng.c at line 390 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	696	696
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
696.                for (x=0; x<=size_max; ++x)
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=861
Status	New

The buffer allocated by <= in mobile-ffmpeg/makepng.c at line 390 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	716	716
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method generate_row(png_bytep row, size_t rowbytes, unsigned int y, int color_type,

```
....
716.                for (x=0; x<=size_max; ++x)
```

Potential Off by One Error in Loops\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=862
Status	New

The buffer allocated by <= in mobile-ffmpeg/mul_fft.c at line 456 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/mul_fft.c	mobile-ffmpeg/mul_fft.c
Line	506	506
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/mul_fft.c
Method mpn_fft_mul_modF_K (mp_ptr *ap, mp_ptr *bp, mp_size_t n, mp_size_t K)

```
....
506.        for (i = 0; i <= k; i++)
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=863
Status	New

The buffer allocated by <= in mobile-ffmpeg/mul_fft.c at line 854 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/mul_fft.c	mobile-ffmpeg/mul_fft.c
Line	875	875
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/mul_fft.c
Method mpn_mul_fft (mp_ptr op, mp_size_t pl,

```
....
875.    for (i = 0; i <= k; i++)
```

Potential Off by One Error in Loops\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=864
Status	New

The buffer allocated by <= in mobile-ffmpeg/rank_reg.c at line 40 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/rank_reg.c	mobile-ffmpeg/rank_reg.c
Line	202	202
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/rank_reg.c
Method int main(int argc,

```
....
202.          for (i = 0; i <= 10; i++) {
```

Potential Off by One Error in Loops\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=865
Status	New

The buffer allocated by <= in mobile-ffmpeg/rdppm.c at line 561 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/rdppm.c	mobile-ffmpeg/rdppm.c
Line	726	726
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/rdppm.c
Method start_input_ppm(j_compress_ptr cinfo, cjpeg_source_ptr sinfo)

```
....
726.      for (val = 0; val <= (long)maxval; val++) {
```

Potential Off by One Error in Loops\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=866
Status	New

The buffer allocated by <= in mobile-ffmpeg/ScrollDetectionFuncs.cpp at line 110 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/ScrollDetectionFuncs.cpp	mobile-ffmpeg/ScrollDetectionFuncs.cpp
Line	135	135
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/ScrollDetectionFuncs.cpp
Method void ScrollDetectionCore (SPixMap* pSrcPixMap, SPixMap* pRefPixMap, int32_t iWidth, int32_t iHeight,

```
....
135.    for (iOffsetAbs = 0; iOffsetAbs <= iMaxAbs; iOffsetAbs++) {
```

Potential Off by One Error in Loops\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=867
Status	New

The buffer allocated by <= in mobile-ffmpeg/tif_pdsdirwrite.c at line 140 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/tif_pdsdirwrite.c	mobile-ffmpeg/tif_pdsdirwrite.c
Line	170	170
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/tif_pdsdirwrite.c
Method TIFFWritePrivateDataSubDirectory(TIFF* tif,

```
....
170.        for (b = 0; b <= pdir_fields_last; b++)
```

Potential Off by One Error in Loops\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=868
Status	New

The buffer allocated by <= in mobile-ffmpeg/tiffmedian.c at line 417 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/tiffmedian.c	mobile-ffmpeg/tiffmedian.c
Line	509	509
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/tiffmedian.c
Method splitbox(Colorbox* ptr)

```
....
509.        for (sum2 = 0, j = i; j <= last; j++)
```

Potential Off by One Error in Loops\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=869
Status	New

The buffer allocated by <= in mobile-ffmpeg/ttgxvar.c at line 1463 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	1570	1570
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method ft_var_load_gvar(TT_Face face)

```
....
1570.        for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=870
Status	New

The buffer allocated by <= in mobile-ffmpeg/ttgxvar.c at line 1463 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	1600	1600
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method ft_var_load_gvar(TT_Face face)

```
....
1600.        for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=871
Status	New

The buffer allocated by <= in mobile-ffmpeg/ttgxvar.c at line 3563 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/ttgxvar.c	mobile-ffmpeg/ttgxvar.c
Line	3579	3579
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/ttgxvar.c
Method tt_delta_interpolate(int p1,

```
....
3579.      for ( i = 0; i <= 1; i++ )
```

Potential Off by One Error in Loops\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=872
Status	New

The buffer allocated by <= in mobile-ffmpeg/tuneup.c at line 2563 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	mobile-ffmpeg/tuneup.c	mobile-ffmpeg/tuneup.c
Line	2590	2590
Object	<=	<=

Code Snippet
File Name mobile-ffmpeg/tuneup.c
Method tune_divexact_1 (void)

```
....
2590.    for (low = 0; low <= 1; low++)
```

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=1060095&projectid=60085&pathid=2402
Status	New

The DecoderInterfaceTest::DecoderBs method in mobile-ffmpeg/DecUT_DecExt.cpp 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	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	150	150
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::DecoderBs (const char* sFileName) {

```
....
150.    ASSERT_TRUE ((pH264File = fopen (filename.c_str(), "rb")) !=
NULL);
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2403
Status	New

The DecoderParseSyntaxTest::DecodeBs method in mobile-ffmpeg/DecUT_ParseSyntax.cpp 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	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	242	242
Object	fopen	fopen

Code Snippet	
File Name	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method	bool DecoderParseSyntaxTest::DecodeBs (const char* sFileName, EDecCase eDecCase) {

```
....
242.    if ((pH264File = fopen (filename.c_str(), "rb")) == NULL)
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2404
Status	New

The DecoderParseSyntaxTest::ParseBs method in mobile-ffmpeg/DecUT_ParseSyntax.cpp 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	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	310	310
Object	fopen	fopen

Code Snippet	
File Name	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method	bool DecoderParseSyntaxTest::ParseBs (const char* sFileName, EDecCase eDecCase) {

```
....
310.    if ((pH264File = fopen (filename.c_str(), "rb")) == NULL)
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2405
Status	New

The floor1_encode method in mobile-ffmpeg/floor1.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	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	889	889
Object	fopen	fopen

Code Snippet	
File Name	mobile-ffmpeg/floor1.c
Method	int floor1_encode(oggpack_buffer *opb,vorbis_block *vb,

```
....
889.            of=fopen(buffer,"a");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2406
Status	New

The floor1_encode method in mobile-ffmpeg/floor1.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	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	913	913
Object	fopen	fopen

Code Snippet	
File Name	mobile-ffmpeg/floor1.c
Method	int floor1_encode(oggpack_buffer *opb,vorbis_block *vb,

```
....
913.              of=fopen(buffer,"a");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2407
Status	New

The *open_output_file method in mobile-ffmpeg/frontend.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	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	614	614
Object	fopen	fopen

Code Snippet

File Name	mobile-ffmpeg/frontend.c
Method	static FILE *open_output_file(char *filename)

```
....
614.          file = fopen(filename, "wb");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2408
Status	New

The main method in mobile-ffmpeg/latticetune.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	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	87	87
Object	fopen	fopen

Code Snippet	
File Name	mobile-ffmpeg/latticetune.c
Method	int main(int argc,char *argv[]){

```
....
87.     in=fopen(argv[2],"r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2409
Status	New

The main method in mobile-ffmpeg/makepng.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	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1833	1833
Object	fopen	fopen

Code Snippet	
File Name	mobile-ffmpeg/makepng.c
Method	main(int argc, char **argv)

```
....
1833.           fp = fopen(arg, "wb");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2410
Status	New

The load_file method in mobile-ffmpeg/makepng.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	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1002	1002
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
1002.        FILE *ip = fopen(name, "rb");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2411
Status	New

The main method in mobile-ffmpeg/png2pnm.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	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	65	65
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method int main (int argc, char *argv[])

```
....
65.             if ((fp_al = fopen (argv[argi], "wb")) == NULL)
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2412
Status	New

The main method in mobile-ffmpeg/png2pnm.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	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	88	88
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method int main (int argc, char *argv[])

```
....
88.         if ((fp_rd = fopen (argv[argi], "rb")) == NULL)
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2413
Status	New

The main method in mobile-ffmpeg/png2pnm.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	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	97	97
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method int main (int argc, char *argv[])

```
....
97.         if ((fp_wr = fopen (argv[argi], "wb")) == NULL)
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2414
Status	New

The main method in mobile-ffmpeg/rdjpgcom.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	mobile-ffmpeg/rdjpgcom.c	mobile-ffmpeg/rdjpgcom.c
Line	485	485
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/rdjpgcom.c
Method main(int argc, char **argv)

```
....
485.      if ((infile = fopen(argv[argn], READ_BINARY)) == NULL) {
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2415
Status	New

The read_quant_tables method in mobile-ffmpeg/rdswitch.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	mobile-ffmpeg/rdswitch.c	mobile-ffmpeg/rdswitch.c
Line	97	97
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/rdswitch.c
Method read_quant_tables(j_compress_ptr cinfo, char *filename, boolean force_baseline)

```
....
97.    if ((fp = fopen(filename, "r")) == NULL) {
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2416
Status	New

The read_scan_script method in mobile-ffmpeg/rdswitch.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	mobile-ffmpeg/rdswitch.c	mobile-ffmpeg/rdswitch.c
Line	195	195
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/rdswitch.c
Method read_scan_script(j_compress_ptr cinfo, char *filename)

```
....
195.    if ((fp = fopen(filename, "r")) == NULL) {
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2417
Status	New

The res0_free_look method in mobile-ffmpeg/res0.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	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	92	92
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/res0.c
Method void res0_free_look(vorbis_look_residue *i){

```
....
92.                 of=fopen(buffer,"a");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2418
Status	New

The **_01class method in mobile-ffmpeg/res0.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	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	457	457
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static long **_01class(vorbis_block *vb,vorbis_look_residue *vl,

```
....
457.          of=fopen(buffer,"a");
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2419
Status	New

The **_2class method in mobile-ffmpeg/res0.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	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	516	516
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static long **_2class(vorbis_block *vb,vorbis_look_residue *vl,int **in,

```
....
516.    of=fopen(buffer,"a");
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2420
Status	New

The oc_state_dump_frame method in mobile-ffmpeg/state.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	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	1097	1097
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/state.c
Method int oc_state_dump_frame(const oc_theora_state *_state,int _frame,

```
....
1097.    fp=fopen(fname,"wb");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2421
Status	New

The main method in mobile-ffmpeg/tiff2pdf.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	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	778	778
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method int main(int argc, char** argv){

```
....
778.              t2p->outputfile = fopen(outfilename, "wb");
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2422
Status	New

The main method in mobile-ffmpeg/transcoder_example.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	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	655	655
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
655.        outfile=fopen(optarg,"wb");
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2423
Status	New

The id_file method in mobile-ffmpeg/transcoder_example.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	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	156	156
Object	fopen	fopen

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
156.      test=fopen(f,"rb");
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2424
Status	New

The testing method in mobile-ffmpeg/abx.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	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	585	585
Object	open	open

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void testing (const stereo_t* A, const stereo_t* B, size_t len, long freq)

```
....
585.      int     fd    = open ( "/dev/dsp", O_WRONLY );
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2425
Status	New

The open_soundcard method in mobile-ffmpeg/ath.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	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	101	101
Object	open	open

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int open_soundcard (

```
....
101.      if ( -1 == (k->fd = open ( k->device, O_WRONLY )) ) {
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2426
Status	New

The play_soundcard method in mobile-ffmpeg/ath.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	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	162	162
Object	open	open

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int play_soundcard (soundcard_t* const k, stereo_t* samples, size_t length)

```
....
162.      if ( fd < 0 ) fd = open ( COOLEDIT_FILE, O_WRONLY | O_CREAT );
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2427
Status	New

The multi_file_test method in mobile-ffmpeg/multi_file_test.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	mobile-ffmpeg/multi_file_test.c	mobile-ffmpeg/multi_file_test.c
Line	141	141
Object	open	open

Code Snippet
File Name mobile-ffmpeg/multi_file_test.c
Method multi_file_test (const char *filename, int *formats, int format_count)

```
....
141.        if ((fd = open (filename, O_RDWR | O_CREAT, S_IRUSR |
S_IWUSR)) < 0)
```

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=1060095&projectid=60085&pathid=2109
Status	New

	Source	Destination
File	mobile-ffmpeg/DecUT_DecExt.cpp	mobile-ffmpeg/DecUT_DecExt.cpp
Line	150	150
Object	pH264File	pH264File

Code Snippet
File Name mobile-ffmpeg/DecUT_DecExt.cpp
Method void DecoderInterfaceTest::DecoderBs (const char* sFileName) {

```
....
150.    ASSERT_TRUE ((pH264File = fopen (filename.c_str(), "rb")) !=
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2110
Status	New

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	242	242
Object	pH264File	pH264File

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method bool DecoderParseSyntaxTest::DecodeBs (const char* sFileName, EDecCase eDecCase) {

```
....
242.    if ((pH264File = fopen (filename.c_str(), "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2111
Status New

	Source	Destination
File	mobile-ffmpeg/DecUT_ParseSyntax.cpp	mobile-ffmpeg/DecUT_ParseSyntax.cpp
Line	310	310
Object	pH264File	pH264File

Code Snippet
File Name mobile-ffmpeg/DecUT_ParseSyntax.cpp
Method bool DecoderParseSyntaxTest::ParseBs (const char* sFileName, EDecCase eDecCase) {

```
....
310.    if ((pH264File = fopen (filename.c_str(), "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2112
Status New

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	889	889
Object	of	of

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int floor1_encode(oggpack_buffer *opb,vorbis_block *vb,

```
....
889.            of=fopen(buffer,"a");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2113
Status	New

	Source	Destination
File	mobile-ffmpeg/floor1.c	mobile-ffmpeg/floor1.c
Line	913	913
Object	of	of

Code Snippet
File Name mobile-ffmpeg/floor1.c
Method int floor1_encode(oggpack_buffer *opb,vorbis_block *vb,

```
....
913.              of=fopen(buffer,"a");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2114
Status	New

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	614	614
Object	file	file

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static FILE *open_output_file(char *filename)

```
....
614.          file = fopen(filename, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2115
Status	New

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	87	87
Object	in	in

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
87.    in=fopen(argv[2],"r");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2116
Status New

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1833	1833
Object	fp	fp

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1833.           fp = fopen(arg, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2117
Status New

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	65	65
Object	fp_al	fp_al

Code Snippet

File Name	mobile-ffmpeg/png2pnm.c
Method	int main (int argc, char *argv[])

```
....
65.             if ((fp_al = fopen (argv[argi], "wb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2118
Status	New

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	88	88
Object	fp_rd	fp_rd

Code Snippet

File Name	mobile-ffmpeg/png2pnm.c
Method	int main (int argc, char *argv[])

```
....
88.         if ((fp_rd = fopen (argv[argi], "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2119
Status	New

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	97	97
Object	fp_wr	fp_wr

Code Snippet

File Name	mobile-ffmpeg/png2pnm.c
Method	int main (int argc, char *argv[])

```
....
97.         if ((fp_wr = fopen (argv[argi], "wb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2120
Status	New

	Source	Destination
File	mobile-ffmpeg/rdjpgcom.c	mobile-ffmpeg/rdjpgcom.c
Line	485	485
Object	infile	infile

Code Snippet
File Name mobile-ffmpeg/rdjpgcom.c
Method main(int argc, char **argv)

```
....
485.      if ((infile = fopen(argv[argn], READ_BINARY)) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2121
Status	New

	Source	Destination
File	mobile-ffmpeg/rdswitch.c	mobile-ffmpeg/rdswitch.c
Line	97	97
Object	fp	fp

Code Snippet
File Name mobile-ffmpeg/rdswitch.c
Method read_quant_tables(j_compress_ptr cinfo, char *filename, boolean force_baseline)

```
....
97.    if ((fp = fopen(filename, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2122
Status	New

	Source	Destination
File	mobile-ffmpeg/rdswitch.c	mobile-ffmpeg/rdswitch.c

Line	195	195
Object	fp	fp

Code Snippet
File Name mobile-ffmpeg/rdswitch.c
Method read_scan_script(j_compress_ptr cinfo, char *filename)

```
....
195.    if ((fp = fopen(filename, "r")) == NULL) {
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2123
Status New

	Source	Destination
File	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	92	92
Object	of	of

Code Snippet
File Name mobile-ffmpeg/res0.c
Method void res0_free_look(vorbis_look_residue *i){

```
....
92.             of=fopen(buffer,"a");
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2124
Status New

	Source	Destination
File	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	457	457
Object	of	of

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static long **_01class(vorbis_block *vb,vorbis_look_residue *vl,

```
....
457.         of=fopen(buffer,"a");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2125
Status	New

	Source	Destination
File	mobile-ffmpeg/res0.c	mobile-ffmpeg/res0.c
Line	516	516
Object	of	of

Code Snippet
File Name mobile-ffmpeg/res0.c
Method static long **_2class(vorbis_block *vb,vorbis_look_residue *vl,int **in,

```
....
516.     of=fopen(buffer,"a");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2126
Status	New

	Source	Destination
File	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	1097	1097
Object	fp	fp

Code Snippet
File Name mobile-ffmpeg/state.c
Method int oc_state_dump_frame(const oc_theora_state *_state,int _frame,

```
....
1097.     fp=fopen(fname,"wb");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2127
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	655	655
Object	outfile	outfile

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
655.        outfile=fopen(optarg,"wb");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2128
Status	New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	156	156
Object	test	test

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method static void id_file(char *f){

```
....
156.      test=fopen(f,"rb");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2129
Status	New

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1002	1002

Object	ip	ip

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
1002.         FILE *ip = fopen(name, "rb");
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2131
Status	New

The system data read by setup in the file mobile-ffmpeg/abx.c at line 525 is potentially exposed by setup found in mobile-ffmpeg/abx.c at line 525.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	531	531
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void setup (int fdd, int samples, long freq)

```
....
531.          perror ("SOUND_PCM_SYNC ioctl failed");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2132
Status	New

The system data read by setup in the file mobile-ffmpeg/abx.c at line 525 is potentially exposed by setup found in mobile-ffmpeg/abx.c at line 525.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	535	535
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void setup (int fdd, int samples, long freq)

```
....
535.          perror ("SOUND_PCM_WRITE_CHANNELS ioctl failed");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2133
Status New

The system data read by setup in the file mobile-ffmpeg/abx.c at line 525 is potentially exposed by setup found in mobile-ffmpeg/abx.c at line 525.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	537	537
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void setup (int fdd, int samples, long freq)

```
....
537.          perror ("unable to set number of channels");
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2134
Status New

The system data read by setup in the file mobile-ffmpeg/abx.c at line 525 is potentially exposed by setup found in mobile-ffmpeg/abx.c at line 525.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c

Line	542	542
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void setup (int fdd, int samples, long freq)

```
....
542.          perror ("SNDCTL_DSP_SETFMT ioctl failed");
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2135
Status	New

The system data read by setup in the file mobile-ffmpeg/abx.c at line 525 is potentially exposed by setup found in mobile-ffmpeg/abx.c at line 525.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	544	544
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void setup (int fdd, int samples, long freq)

```
....
544.          perror ("unable to set data format");
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2136
Status	New

The system data read by setup in the file mobile-ffmpeg/abx.c at line 525 is potentially exposed by setup found in mobile-ffmpeg/abx.c at line 525.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	548	548
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/abx.c
Method void setup (int fdd, int samples, long freq)

```
....
548.          perror ("SNDCTL_DSP_SPEED ioctl failed");
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2137
Status New

The system data read by open_soundcard in the file mobile-ffmpeg/ath.c at line 88 is potentially exposed by open_soundcard found in mobile-ffmpeg/ath.c at line 88.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	102	102
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int open_soundcard (

```
....
102.          perror("opening of audio device failed");
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2138
Status New

The system data read by main in the file mobile-ffmpeg/frontend.c at line 704 is potentially exposed by main found in mobile-ffmpeg/frontend.c at line 704.

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	820	820
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/frontend.c

Method	int main(int argc, char **argv)

```
....
820.              perror("error while writing to output file");
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2139
Status	New

The system data read by main in the file mobile-ffmpeg/frontend.c at line 704 is potentially exposed by main found in mobile-ffmpeg/frontend.c at line 704.

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	856	856
Object	perror	perror

Code Snippet	
File Name	mobile-ffmpeg/frontend.c
Method	int main(int argc, char **argv)

```
....
856.              perror("error while writing to output file");
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2140
Status	New

The system data read by *open_output_file in the file mobile-ffmpeg/frontend.c at line 605 is potentially exposed by *open_output_file found in mobile-ffmpeg/frontend.c at line 605.

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	619	619
Object	perror	perror

Code Snippet	
File Name	mobile-ffmpeg/frontend.c
Method	static FILE *open_output_file(char *filename)

```
....
619.          perror("Failed to open output file");
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2141
Status	New

The system data read by load_file in the file mobile-ffmpeg/makepng.c at line 996 is potentially exposed by load_file found in mobile-ffmpeg/makepng.c at line 996.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1019	1019
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
1019.              perror(name);
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2142
Status	New

The system data read by load_file in the file mobile-ffmpeg/makepng.c at line 996 is potentially exposed by load_file found in mobile-ffmpeg/makepng.c at line 996.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1030	1030
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
1030.                perror("temporary file");
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2143
Status	New

The system data read by load_file in the file mobile-ffmpeg/makepng.c at line 996 is potentially exposed by load_file found in mobile-ffmpeg/makepng.c at line 996.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1058	1058
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
1058.                            perror("temporary file");
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2144
Status	New

The system data read by load_file in the file mobile-ffmpeg/makepng.c at line 996 is potentially exposed by load_file found in mobile-ffmpeg/makepng.c at line 996.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1083	1083
Object	perror	perror

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
1083.           perror(name);
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2145
Status	New

The system data read by main in the file mobile-ffmpeg/test_opus_encode.c at line 637 is potentially exposed by main found in mobile-ffmpeg/test_opus_encode.c at line 637.

	Source	Destination
File	mobile-ffmpeg/test_opus_encode.c	mobile-ffmpeg/test_opus_encode.c
Line	648	684
Object	getenv	fprintf

Code Snippet
File Name mobile-ffmpeg/test_opus_encode.c
Method int main(int _argc, char **_argv)

```
....
648.     env_seed=getenv("SEED");
....
684.     if(env_used)fprintf(stderr,"  Random seed set from the
environment (SEED=%s).\n", env_seed);
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2146
Status	New

The system data read by open_soundcard in the file mobile-ffmpeg/ath.c at line 88 is potentially exposed by open_soundcard found in mobile-ffmpeg/ath.c at line 88.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	107	107
Object	errno	fprintf

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int open_soundcard (

```
....
107.          fprintf ( stderr, "%s: SOUND_PCM_SYNC ioctl failed: %s\n",
k->device, strerror (errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2147
Status	New

The system data read by open_soundcard in the file mobile-ffmpeg/ath.c at line 88 is potentially exposed by open_soundcard found in mobile-ffmpeg/ath.c at line 88.

	Source	Destination
File	mobile-ffmpeg/ath.c	mobile-ffmpeg/ath.c
Line	113	113
Object	errno	fprintf

Code Snippet
File Name mobile-ffmpeg/ath.c
Method int open_soundcard (

```
....
113.        fprintf ( stderr, "%s: SOUND_PCM_WRITE_CHANNELS (%d) ioctl
failed: %s\n" , k->device, channels, strerror (errno) );
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2148
Status	New

The system data read by main in the file mobile-ffmpeg/makepng.c at line 1678 is potentially exposed by main found in mobile-ffmpeg/makepng.c at line 1678.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1836	1836
Object	errno	fprintf

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1836.               fprintf(stderr, "%s: %s: could not open\n", arg,
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2149
Status	New

The system data read by multi_file_test in the file mobile-ffmpeg/multi_file_test.c at line 130 is potentially exposed by multi_file_test found in mobile-ffmpeg/multi_file_test.c at line 130.

	Source	Destination
File	mobile-ffmpeg/multi_file_test.c	mobile-ffmpeg/multi_file_test.c
Line	142	165
Object	errno	printf

Code Snippet
File Name mobile-ffmpeg/multi_file_test.c
Method multi_file_test (const char *filename, int *formats, int format_count)

```
....
142.        {     printf ("\n\nLine %d: open failed : %s\n", __LINE__,
strerror (errno)) ;
....
165.              {     printf ("\n\nLine %d: lseek failed : %s\n",
__LINE__, strerror (errno)) ;
```

Exposure of System Data to Unauthorized Control Sphere\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2150
Status	New

The system data read by multi_file_test in the file mobile-ffmpeg/multi_file_test.c at line 130 is potentially exposed by multi_file_test found in mobile-ffmpeg/multi_file_test.c at line 130.

	Source	Destination
File	mobile-ffmpeg/multi_file_test.c	mobile-ffmpeg/multi_file_test.c
Line	165	165
Object	errno	printf

Code Snippet
File Name mobile-ffmpeg/multi_file_test.c

Method	multi_file_test (const char *filename, int *formats, int format_count)

```
....
165.              {     printf ("\n\nLine %d: lseek failed : %s\n",
__LINE__, strerror (errno)) ;
```

Exposure of System Data to Unauthorized Control Sphere\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2151
Status	New

The system data read by multi_file_test in the file mobile-ffmpeg/multi_file_test.c at line 130 is potentially exposed by multi_file_test found in mobile-ffmpeg/multi_file_test.c at line 130.

	Source	Destination
File	mobile-ffmpeg/multi_file_test.c	mobile-ffmpeg/multi_file_test.c
Line	142	142
Object	errno	printf

Code Snippet	
File Name	mobile-ffmpeg/multi_file_test.c
Method	multi_file_test (const char *filename, int *formats, int format_count)

```
....
142.        {     printf ("\n\nLine %d: open failed : %s\n", __LINE__,
strerror (errno)) ;
```

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=1060095&projectid=60085&pathid=2577
Status	New

	Source	Destination
File	mobile-ffmpeg/adaptmap.c	mobile-ffmpeg/adaptmap.c
Line	2855	2855
Object	sizeof	sizeof

Code Snippet	
File Name	mobile-ffmpeg/adaptmap.c

Method	pixLinearTRCTiled(PIX *pixd,

```
....
2855.      if ((iaa = (l_int32 **)LEPT_CALLOC(256, sizeof(l_int32 *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2578
Status	New

	Source	Destination
File	mobile-ffmpeg/ccbord.c	mobile-ffmpeg/ccbord.c
Line	327	327
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/ccbord.c
Method ccbaCreate(PIX *pixs,

```
....
327.      if ((ccba->ccb = (CCBORD **)LEPT_CALLOC(n, sizeof(CCBORD *)))
== NULL) {
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2579
Status	New

	Source	Destination
File	mobile-ffmpeg/ccbord.c	mobile-ffmpeg/ccbord.c
Line	500	500
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/ccbord.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
500.                                  sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2580
Status	New

	Source	Destination
File	mobile-ffmpeg/ccbord.c	mobile-ffmpeg/ccbord.c
Line	501	501
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/ccbord.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
501.                                    2 * sizeof(CCBORD *) * ccba-
>nalloc)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2581
Status	New

	Source	Destination
File	mobile-ffmpeg/compare.c	mobile-ffmpeg/compare.c
Line	1950	1950
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/compare.c
Method pixaComparePhotoRegionsByHisto(PIXA *pixa,

```
....
1950.      if ((n3a = (NUMAA **)LEPT_CALLOC(nim, sizeof(NUMAA *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2582
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	176	176
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaCreate(l_int32 n)

```
....
176.      pixa->pix = (PIX **)LEPT_CALLOC(n, sizeof(PIX *));
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2583
Status New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	612	612
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaExtendArrayToSize(PIXA *pixa,

```
....
612.                                    sizeof(PIX *) * pixa->nalloc,
```

Use of Sizeof On a Pointer Type\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2584
Status New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	613	613
Object	sizeof	sizeof

Code Snippet

File Name	mobile-ffmpeg/pixabasic.c
Method	pixaExtendArrayToSize(PIXA *pixa,

```
....
613.                                    size * sizeof(PIX *))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2585
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	1211	1211
Object	sizeof	sizeof

Code Snippet

File Name	mobile-ffmpeg/pixabasic.c
Method	pixaGetLinePtrs(PIXA *pixa,

```
....
1211.       if ((lineset = (void ***)LEPT_CALLOC(n, sizeof(void **))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2586
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	1838	1838
Object	sizeof	sizeof

Code Snippet

File Name	mobile-ffmpeg/pixabasic.c
Method	pixaaCreate(l_int32 n)

```
....
1838.       if ((paa->pixa = (PIXA **)LEPT_CALLOC(n, sizeof(PIXA *))) ==
NULL) {
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2587
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2024	2024
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaExtendArray(PIXAA *paa)

```
....
2024.                                   sizeof(PIXA *) * paa->nalloc,
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2588
Status	New

	Source	Destination
File	mobile-ffmpeg/pixabasic.c	mobile-ffmpeg/pixabasic.c
Line	2025	2025
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/pixabasic.c
Method pixaaExtendArray(PIXAA *paa)

```
....
2025.                                   2 * sizeof(PIXA *) * paa->nalloc))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2589
Status	New

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	307	307
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method BOOL png2pnm (FILE *png_file, FILE *pnm_file, FILE *alpha_file,

```
....
307.          malloc ((size_t) height * sizeof (png_byte *))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2590
Status New

	Source	Destination
File	mobile-ffmpeg/tif_ojpeg.c	mobile-ffmpeg/tif_ojpeg.c
Line	1260	1260
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/tif_ojpeg.c
Method OJPEGWriteHeaderInfo(TIFF* tif)

```
....
1260.                    sp-
>subsampling_convert_ycbcrimage=_TIFFmalloc(sp-
>subsampling_convert_ycbcrimagelen*sizeof(uint8*));
```

Use of Sizeof On a Pointer Type\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2591
Status New

	Source	Destination
File	mobile-ffmpeg/tiffmedian.c	mobile-ffmpeg/tiffmedian.c
Line	237	237
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/tiffmedian.c
Method main(int argc, char* argv[])

```
....
237.        ColorCells = (C_cell **)_TIFFmalloc(C_LEN*C_LEN*C_LEN*sizeof
(C_cell*));
```

Use of Sizeof On a Pointer Type\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2592
Status New

	Source	Destination
File	mobile-ffmpeg/tiffmedian.c	mobile-ffmpeg/tiffmedian.c
Line	238	238
Object	sizeof	sizeof

Code Snippet
File Name mobile-ffmpeg/tiffmedian.c
Method main(int argc, char* argv[])

```
....
238.        _TIFFmemset(ColorCells, 0, C_LEN*C_LEN*C_LEN*sizeof
(C_cell*));
```

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=1060095&projectid=60085&pathid=886
Status New

The size of the buffer used by readwave in name, at line 947 of mobile-ffmpeg/abx.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 1207 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination

File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1207	949
Object	argv	name

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1207.  int  main ( int argc, char** argv )
```

File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
949.       char*           command = malloc (2*strlen(name) + 512);
```

Heuristic Buffer Overflow malloc\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=887
Status	New

The size of the buffer used by readwave in name, at line 947 of mobile-ffmpeg/abx.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 1207 of mobile-ffmpeg/abx.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/abx.c	mobile-ffmpeg/abx.c
Line	1207	950
Object	argv	name

Code Snippet
File Name mobile-ffmpeg/abx.c
Method int main (int argc, char** argv)

```
....
1207.  int  main ( int argc, char** argv )
```

File Name mobile-ffmpeg/abx.c
Method int readwave (stereo_t* buff, size_t maxlen, const char* name, size_t* len)

```
....
950.       char*           name_q  = malloc (2*strlen(name) + 128);
```

Heuristic Buffer Overflow malloc\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=888
Status	New

The size of the buffer used by main in PNG_IMAGE_SIZE, at line 748 of mobile-ffmpeg/genpng.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 748 of mobile-ffmpeg/genpng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/genpng.c	mobile-ffmpeg/genpng.c
Line	748	801
Object	argv	PNG_IMAGE_SIZE

Code Snippet
File Name mobile-ffmpeg/genpng.c
Method main(int argc, const char **argv)

```
....
748.  main(int argc, const char **argv)
....
801.        buffer = malloc(PNG_IMAGE_SIZE(image));
```

Heuristic Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=889
Status	New

The size of the buffer used by main in image, at line 748 of mobile-ffmpeg/genpng.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 748 of mobile-ffmpeg/genpng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/genpng.c	mobile-ffmpeg/genpng.c
Line	748	801
Object	argv	image

Code Snippet
File Name mobile-ffmpeg/genpng.c
Method main(int argc, const char **argv)

```
....
748.  main(int argc, const char **argv)
....
801.        buffer = malloc(PNG_IMAGE_SIZE(image));
```

Heuristic Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=890
Status	New

The size of the buffer used by exchange in top, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	215
Object	argc	top

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
215.        char *new_str = malloc (top + 1);
```

Heuristic Buffer Overflow malloc\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=891
Status	New

The size of the buffer used by exchange in top, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c

Line	1205	215
Object	argv	top

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
215.        char *new_str = malloc (top + 1);
```

Heuristic Buffer Overflow malloc\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=892
Status	New

The size of the buffer used by exchange in top, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	215
Object	getenv	top

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c
Method exchange (

```
....
215.        char *new_str = malloc (top + 1);
```

Heuristic Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=893
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	215
Object	argc	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
215.        char *new_str = malloc (top + 1);
```

Heuristic Buffer Overflow malloc\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=894
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.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 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1205	215
Object	argv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method main (

```
....
1205.    char **argv
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
215.        char *new_str = malloc (top + 1);
```

Heuristic Buffer Overflow malloc\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=895
Status	New

The size of the buffer used by exchange in BinaryExpr, at line 192 of mobile-ffmpeg/getopt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _getopt_initialize passes to getenv, at line 276 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	291	215
Object	getenv	BinaryExpr

Code Snippet

File Name mobile-ffmpeg/getopt.c

Method _getopt_initialize (

```
....
291.    d->__posixly_correct = !!getenv ("POSIXLY_CORRECT");
```

File Name mobile-ffmpeg/getopt.c

Method exchange (

```
....
215.        char *new_str = malloc (top + 1);
```

Heuristic Buffer Overflow malloc\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=896
Status	New

The size of the buffer used by _getopt_initialize in __nonoption_flags_max_len, at line 276 of mobile-ffmpeg/getopt.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 argc, at line 1203 of mobile-ffmpeg/getopt.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1204	325
Object	argc	__nonoption_flags_max_len

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1204.    int argc,
```

File Name mobile-ffmpeg/getopt.c
Method _getopt_initialize (

```
....
325.              (char *) malloc (d->__nonoption_flags_max_len);
```

Heuristic Buffer Overflow malloc\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=897
Status New

The size of the buffer used by write_png in rowbytes, at line 770 of mobile-ffmpeg/makepng.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 1678 of mobile-ffmpeg/makepng.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1678	955
Object	argv	rowbytes

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1678.  main(int argc, char **argv)
```

File Name	mobile-ffmpeg/makepng.c
Method	write_png(const char **name, FILE *fp, int color_type, int bit_depth,

```
....
955.            row = malloc(rowbytes);
```

Heuristic Buffer Overflow malloc\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=898
Status	New

The size of the buffer used by fetch_and_process_video in framelength, at line 489 of mobile-ffmpeg/transcoder_example.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that id_file passes to stdin, at line 145 of mobile-ffmpeg/transcoder_example.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	154	549
Object	stdin	framelength

Code Snippet

File Name	mobile-ffmpeg/transcoder_example.c
Method	static void id_file(char *f){

```
....
154.      test=stdin;
```

File Name	mobile-ffmpeg/transcoder_example.c
Method	int fetch_and_process_video(FILE *video,ogg_page *videopage,

```
....
549.          vp3frame[i] = malloc(framelength);
```

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=1060095&projectid=60085&pathid=830
Status	New

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c
Line	1215	1215
Object	getopt	getopt

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method main (

```
....
1215.         c = getopt (argc, argv, "abc:d:0123456789");
```

Inconsistent Implementations\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=831
Status New

	Source	Destination
File	mobile-ffmpeg/tiff2pdf.c	mobile-ffmpeg/tiff2pdf.c
Line	619	619
Object	getopt	getopt

Code Snippet
File Name mobile-ffmpeg/tiff2pdf.c
Method int main(int argc, char** argv){

```
....
619.                (c = getopt(argc, argv,
```

Inconsistent Implementations\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=832
Status New

	Source	Destination
File	mobile-ffmpeg/tiff2ps.c	mobile-ffmpeg/tiff2ps.c
Line	255	255
Object	getopt	getopt

Code Snippet

File Name	mobile-ffmpeg/tiff2ps.c
Method	main(int argc, char* argv[])

```
....
255.        while ((c = getopt(argc, argv,
"b:d:h:H:W:L:i:w:l:o:O:P:C:r:t:acemxyzps1238DT")) != -1)
```

Inconsistent Implementations\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=833
Status	New

	Source	Destination
File	mobile-ffmpeg/tiffcp.c	mobile-ffmpeg/tiffcp.c
Line	176	176
Object	getopt	getopt

Code Snippet	
File Name	mobile-ffmpeg/tiffcp.c
Method	main(int argc, char* argv[])

```
....
176.        while ((c = getopt(argc, argv,
",:b:c:f:l:o:p:r:w:aistBLMC8x")) != -1)
```

Inconsistent Implementations\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=834
Status	New

	Source	Destination
File	mobile-ffmpeg/tiffmedian.c	mobile-ffmpeg/tiffmedian.c
Line	130	130
Object	getopt	getopt

Code Snippet	
File Name	mobile-ffmpeg/tiffmedian.c
Method	main(int argc, char* argv[])

```
....
130.        while ((c = getopt(argc, argv, "c:C:r:f")) != -1)
```

Inconsistent Implementations\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=835
Status	New

	Source	Destination
File	mobile-ffmpeg/tuneup.c	mobile-ffmpeg/tuneup.c
Line	3045	3045
Object	getopt	getopt

Code Snippet
File Name mobile-ffmpeg/tuneup.c
Method main (int argc, char *argv[])

```
....
3045.    while ((opt = getopt(argc, argv, "f:o:p:t")) != EOF)
```

Inconsistent Implementations\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=836
Status	New

	Source	Destination
File	mobile-ffmpeg/cli.c	mobile-ffmpeg/cli.c
Line	212	212
Object	getopt_long	getopt_long

Code Snippet
File Name mobile-ffmpeg/cli.c
Method cmdline_opts_t* cmdline_opts_parse(const kvz_api *const api, int argc, char *argv[])

```
....
212.      int c = getopt_long(argc, argv, short_options, long_options,
&long_options_index);
```

Inconsistent Implementations\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=837
Status	New

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	349	349
Object	getopt_long	getopt_long

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method static void parse_args(int argc, char **argv, twolame_options * encopts)

```
....
349.        while ((ch = getopt_long(argc, argv, shortopts, longopts,
NULL)) != -1) {
```

Inconsistent Implementations\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=838
Status New

	Source	Destination
File	mobile-ffmpeg/getopt1.c	mobile-ffmpeg/getopt1.c
Line	148	148
Object	getopt_long	getopt_long

Code Snippet
File Name mobile-ffmpeg/getopt1.c
Method main (

```
....
148.        c = getopt_long (argc, argv, "abc:d:0123456789",
```

Inconsistent Implementations\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=839
Status New

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	652	652
Object	getopt_long	getopt_long

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int main(int argc,char *argv[]){

```
....
652.
while((c=getopt_long(argc,argv,optstring,options,&long_option_index))!=E
OF){
```

Potential Path Traversal

Query Path:
CPP\Cx\CPP Low Visibility\Potential Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description

Potential Path Traversal\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2152
Status	New

Method main at line 704 of mobile-ffmpeg/frontend.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in *open_output_file at line 605 of mobile-ffmpeg/frontend.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/frontend.c	mobile-ffmpeg/frontend.c
Line	704	614
Object	argv	filename

Code Snippet
File Name mobile-ffmpeg/frontend.c
Method int main(int argc, char **argv)

```
....
704.  int main(int argc, char **argv)
```

File Name mobile-ffmpeg/frontend.c
Method static FILE *open_output_file(char *filename)

```
....
614.          file = fopen(filename, "wb");
```

Potential Path Traversal\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2153
Status	New

Method main at line 38 of mobile-ffmpeg/latticetune.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 38 of mobile-ffmpeg/latticetune.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/latticetune.c	mobile-ffmpeg/latticetune.c
Line	38	87
Object	argv	argv

Code Snippet
File Name mobile-ffmpeg/latticetune.c
Method int main(int argc,char *argv[]){

```
....
38.  int main(int argc,char *argv[]){
....
87.    in=fopen(argv[2],"r");
```

Potential Path Traversal\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2154
Status	New

Method main at line 1678 of mobile-ffmpeg/makepng.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 1678 of mobile-ffmpeg/makepng.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	1678	1833
Object	argv	arg

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method main(int argc, char **argv)

```
....
1678.  main(int argc, char **argv)
....
1833.           fp = fopen(arg, "wb");
```

Potential Path Traversal\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2155
Status	New

Method main at line 41 of mobile-ffmpeg/png2pnm.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 41 of mobile-ffmpeg/png2pnm.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	41	65
Object	argv	argv

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method int main (int argc, char *argv[])

```
....
41.  int main (int argc, char *argv[])
....
65.            if ((fp_al = fopen (argv[argi], "wb")) == NULL)
```

Potential Path Traversal\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2156
Status	New

Method main at line 41 of mobile-ffmpeg/png2pnm.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 41 of mobile-ffmpeg/png2pnm.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	41	88
Object	argv	argv

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method int main (int argc, char *argv[])

```
....
41.  int main (int argc, char *argv[])
....
88.        if ((fp_rd = fopen (argv[argi], "rb")) == NULL)
```

Potential Path Traversal\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2157
Status	New

Method main at line 41 of mobile-ffmpeg/png2pnm.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 41 of mobile-ffmpeg/png2pnm.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/png2pnm.c	mobile-ffmpeg/png2pnm.c
Line	41	97
Object	argv	argv

Code Snippet
File Name mobile-ffmpeg/png2pnm.c
Method int main (int argc, char *argv[])

```
....
41.  int main (int argc, char *argv[])
....
97.         if ((fp_wr = fopen (argv[argi], "wb")) == NULL)
```

Potential Path Traversal\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2158
Status	New

Method main at line 449 of mobile-ffmpeg/rdjpgcom.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in main at line 449 of mobile-ffmpeg/rdjpgcom.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/rdjpgcom.c	mobile-ffmpeg/rdjpgcom.c
Line	449	485
Object	argv	argv

Code Snippet
File Name mobile-ffmpeg/rdjpgcom.c
Method main(int argc, char **argv)

```
....
449.  main(int argc, char **argv)
....
485.      if ((infile = fopen(argv[argn], READ_BINARY)) == NULL) {
```

Potential Path Traversal\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=2159
Status	New

Method main at line 609 of mobile-ffmpeg/transcoder_example.c gets user input from the argv element. This element's value then flows through the code and is eventually used in a file path for local disk access in id_file at line 145 of mobile-ffmpeg/transcoder_example.c. This may cause a Path Traversal vulnerability.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	609	156
Object	argv	f

Code Snippet

File Name mobile-ffmpeg/transcoder_example.c

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

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

File Name mobile-ffmpeg/transcoder_example.c

Method static void id_file(char *f){

```
....
156.      test=fopen(f,"rb");
```

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=1060095&projectid=60085&pathid=899
Status	New

	Source	Destination
File	mobile-ffmpeg/getopt.c	mobile-ffmpeg/getopt.c

Line	514	514
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/getopt.c
Method _getopt_internal_r (

```
....
514.                    + (longopts != NULL && argv[d->optind][1] == '-
'));
```

Arithmenic Operation On Boolean\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=900
Status New

	Source	Destination
File	mobile-ffmpeg/mul_fft.c	mobile-ffmpeg/mul_fft.c
Line	246	246
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/mul_fft.c
Method mpn_fft_mul_2exp_modF (mp_ptr r, mp_srcptr a, mp_bitcnt_t d, mp_size_t n)

```
....
246.        r = r + m + (rd == 0);
```

Arithmenic Operation On Boolean\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=901
Status New

	Source	Destination
File	mobile-ffmpeg/ttinterp.c	mobile-ffmpeg/ttinterp.c
Line	1472	1472
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/ttinterp.c
Method TT_DotFix14(FT_Int32 ax,

```
....
1472.       hi1 = ( m >> 16 ) + ( (FT_Int32)l >> 31 ) + ( lo1 < l );
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=902
Status	New

	Source	Destination
File	mobile-ffmpeg/ttinterp.c	mobile-ffmpeg/ttinterp.c
Line	1479	1479
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/ttinterp.c
Method TT_DotFix14(FT_Int32 ax,

```
....
1479.       hi2 = ( m >> 16 ) + ( (FT_Int32)l >> 31 ) + ( lo2 < l );
```

Arithmenic Operation On Boolean\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=903
Status	New

	Source	Destination
File	mobile-ffmpeg/ttinterp.c	mobile-ffmpeg/ttinterp.c
Line	1483	1483
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/ttinterp.c
Method TT_DotFix14(FT_Int32 ax,

```
....
1483.       hi = hi1 + hi2 + ( lo < lo1 );
```

Arithmenic Operation On Boolean\Path 6:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=904
Status	New

	Source	Destination
File	mobile-ffmpeg/ttinterp.c	mobile-ffmpeg/ttinterp.c
Line	1488	1488
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/ttinterp.c
Method TT_DotFix14(FT_Int32 ax,

```
....
1488.       hi += s + ( l < lo );
```

Arithmenic Operation On Boolean\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=905
Status	New

	Source	Destination
File	mobile-ffmpeg/tuneup.c	mobile-ffmpeg/tuneup.c
Line	2172	2172
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name mobile-ffmpeg/tuneup.c
Method tune_powm_sec (void)

```
....
2172.         nbits = nbits_next + (nbits_next == nbits);
```

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=1060095&projectid=60085&pathid=884
Status	New

The size of the buffer used by fetch_and_process_video in framelength, at line 489 of mobile-ffmpeg/transcoder_example.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fetch_and_process_video passes to Address, at line 489 of mobile-ffmpeg/transcoder_example.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/transcoder_example.c	mobile-ffmpeg/transcoder_example.c
Line	544	549
Object	Address	framelength

Code Snippet
File Name mobile-ffmpeg/transcoder_example.c
Method int fetch_and_process_video(FILE *video,ogg_page *videopage,

```
....
544.          ret=fread(&framelength, sizeof(int), 1, video);
....
549.          vp3frame[i] = malloc(framelength);
```

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=1060095&projectid=60085&pathid=885
Status	New

The size of the buffer used by oc_state_dump_frame in "%08i%s.png", at line 1068 of mobile-ffmpeg/state.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that oc_state_dump_frame passes to "%08i%s.png", at line 1068 of mobile-ffmpeg/state.c, to overwrite the target buffer.

	Source	Destination
File	mobile-ffmpeg/state.c	mobile-ffmpeg/state.c
Line	1096	1096
Object	"%08i%s.png"	"%08i%s.png"

Code Snippet

File Name	mobile-ffmpeg/state.c
Method	int oc_state_dump_frame(const oc_theora_state *_state,int _frame,

```
....
1096.    sprintf(fname,"%08i%s.png",(int)(iframe+pframe),_suf);
```

Insecure Temporary File

Query Path:
CPP\Cx\CPP Low Visibility\Insecure Temporary File Version:0

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insecure Temporary File\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=906
Status	New

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	998	998
Object	tmpfile	tmpfile

Code Snippet

File Name	mobile-ffmpeg/makepng.c
Method	load_file(png_const_charp name, png_bytepp result)

```
....
998.     FILE *fp = tmpfile();
```

Leaving Temporary Files

Query Path:
CPP\Cx\CPP Low Visibility\Leaving Temporary Files Version:0

Categories

OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Leaving Temporary Files\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1060095&projectid=60085&pathid=907
Status	New

The application generates a temporary file tmpfile, in the load_file method at mobile-ffmpeg/makepng.c:996. This temporary file is never removed, and will remain in the TEMP folder indefinitely.

	Source	Destination
File	mobile-ffmpeg/makepng.c	mobile-ffmpeg/makepng.c
Line	998	998
Object	tmpfile	tmpfile

Code Snippet
File Name mobile-ffmpeg/makepng.c
Method load_file(png_const_charp name, png_bytepp result)

```
....
998.     FILE *fp = tmpfile();
```

Buffer Overflow Indexes

Risk

What might happen

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

Cause

How does it happen

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

General Recommendations

How to avoid it

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

Source Code Examples

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow 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 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

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));
    }
}
```

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

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

Improper Null Termination

Weakness ID: 170 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

The software does not terminate or incorrectly terminates a string or array with a null character or equivalent terminator.

Extended Description

Null termination errors frequently occur in two different ways. An off-by-one error could cause a null to be written out of bounds, leading to an overflow. Or, a program could use a strncpy() function call incorrectly, which prevents a null terminator from being added at all. Other scenarios are possible.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Platform Notes

Conceptually, this does not just apply to the C language; any language or representation that involves a terminator could have this type of problem.

Common Consequences

Scope	Effect
Confidentiality Integrity	The case of an omitted null character is the most dangerous of the possible issues. This will almost certainly result in information disclosure, and possibly a buffer overflow condition, which may be exploited to execute arbitrary code.
Confidentiality Integrity Availability	If a null character is omitted from a string, then most string-copying functions will read data until they locate a null character, even outside of the intended boundaries of the string. This could: • cause a crash due to a segmentation fault • cause sensitive adjacent memory to be copied and sent to an outsider • trigger a buffer overflow when the copy is bering written to a fixed-size buffer
Integrity Availability	Misplaced null characters may result in any number of security problems. The biggest issue is a subset of buffer overflow, and write-what-where conditions, where data corruption occurs from the writing of a null character over valid data, or even instructions. A randomly placed null character may put the system into an undefined state, and therefore make it prone to crashing. A misplaced null character may corrupt other data in memory
Access Control	Should the null character corrupt the process flow, or affect a flag controlling access, it may lead to logical errors which allow for the execution of arbitrary code.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following code reads from cfgfile and copies the input into inputbuf using strcpy(). The code mistakenly assumes that inputbuf will always contain a NULL terminator.

(Bad Code)

Example Language: **C**

```
#define MAXLEN 1024
...
char *pathbuf[MAXLEN];
...
read(cfgfile,inputbuf,MAXLEN); //does not null terminate
strcpy(pathbuf,input_buf); //requires null terminated input
...
```

The code above will behave correctly if the data read from cfgfile is null terminated on disk as expected. But if an attacker is able to modify this input so that it does not contain the expected NULL character, the call to strcpy() will continue copying from memory until it encounters an arbitrary NULL character. This will likely overflow the destination buffer and, if the attacker can control the contents of memory immediately following inputbuf, can leave the application susceptible to a buffer overflow attack.

Example 2

In the following code, readlink() expands the name of a symbolic link stored in the buffer path so that the buffer filename contains the absolute path of the file referenced by the symbolic link. The length of the resulting value is then calculated using strlen().

(Bad Code)

Example Language: **C**

```
char buf[MAXPATH];
...
readlink(path, buf, MAXPATH);
int length = strlen(filename);
...
```

The code above will not behave correctly because the value read into buf by readlink() will not be null terminated. In testing, vulnerabilities like this one might not be caught because the unused contents of buf and the memory immediately following it may be NULL, thereby causing strlen() to appear as if it is behaving correctly. However, in the wild strlen() will continue traversing memory until it encounters an arbitrary NULL character on the stack, which results in a value of length that is much larger than the size of buf and may cause a buffer overflow in subsequent uses of this value. Buffer overflows aside, whenever a single call to readlink() returns the same value that has been passed to its third argument, it is impossible to know whether the name is precisely that many bytes long, or whether readlink() has truncated the name to avoid overrunning the buffer. Traditionally, strings are represented as a region of memory containing data terminated with a NULL character. Older string-handling methods frequently rely on this NULL character to determine the length of the string. If a buffer that does not contain a NULL terminator is passed to one of these functions, the function will read past the end of the buffer. Malicious users typically exploit this type of vulnerability by injecting data with unexpected size or content into the application. They may provide the malicious input either directly as input to the program or indirectly by modifying application resources, such as configuration files. In the event that an attacker causes the application to read beyond the bounds of a buffer, the attacker may be able use a resulting buffer overflow to inject and execute arbitrary code on the system.

Example 3

While the following example is not exploitable, it provides a good example of how nulls can be omitted or misplaced, even when "safe" functions are used:

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <string.h>

int main() {

char longString[] = "String signifying nothing";
char shortString[16];

strncpy(shortString, longString, 16);
printf("The last character in shortString is: %c %1$x\n", shortString[15]);
return (0);
}
```

The above code gives the following output: The last character in shortString is: l 6c So, the shortString array does not end in a NULL character, even though the "safe" string function strncpy() was used.

Observed Examples

Reference	Description
CVE-2000-0312	Attacker does not null-terminate argv[] when invoking another program.
CVE-2003-0777	Interrupted step causes resultant lack of null termination.
CVE-2004-1072	Fault causes resultant lack of null termination, leading to buffer expansion.
CVE-2001-1389	Multiple vulnerabilities related to improper null termination.
CVE-2003-0143	Product does not null terminate a message buffer after snprintf-like call, leading to overflow.

Potential Mitigations

Phase: Requirements

Use a language that is not susceptible to these issues. However, be careful of null byte interaction errors (CWE-626) with lower-level constructs that may be written in a language that is susceptible.

Phase: Implementation

Ensure that all string functions used are understood fully as to how they append null characters. Also, be wary of off-by-one errors when appending nulls to the end of strings.

Phase: Implementation

If performance constraints permit, special code can be added that validates null-termination of string buffers, this is a rather naive and error-prone solution.

Phase: Implementation

Switch to bounded string manipulation functions. Inspect buffer lengths involved in the buffer overrun trace reported with the defect.

Phase: Implementation

Add code that fills buffers with nulls (however, the length of buffers still needs to be inspected, to ensure that the non null-terminated string is not written at the physical end of the buffer).

Weakness Ordinalities

Ordinality	Description
Resultant	*(where the weakness is typically related to the presence of some other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	169	Technology-Specific	**Development**

			Special Elements	**Concepts (primary)699**
ChildOf	Weakness Class	707	Improper Enforcement of Message or Data Structure	**Research Concepts (primary)1000**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	741	CERT C Secure Coding Section 07 - Characters and Strings (STR)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	748	CERT C Secure Coding Section 50 - POSIX (POS)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Research Concepts1000
CanPrecede	Weakness Variant	126	Buffer Over-read	Research Concepts1000
PeerOf	Weakness Base	463	Deletion of Data Structure Sentinel	Research Concepts1000
PeerOf	Weakness Base	464	Addition of Data Structure Sentinel	Research Concepts1000
CanAlsoBe	Weakness Variant	147	Improper Neutralization of Input Terminators	Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Base	193	Off-by-one Error	Research Concepts1000
CanFollow	Weakness Class	682	Incorrect Calculation	Research Concepts1000

Relationship Notes

Factors: this is usually resultant from other weaknesses such as off-by-one errors, but it can be primary to boundary condition violations such as buffer overflows. In buffer overflows, it can act as an expander for assumed-immutable data.

Overlaps missing input terminator.

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Improper Null Termination
7 Pernicious Kingdoms			String Termination Error
CLASP			Miscalculated null termination
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service
CERT C Secure Coding	POS30-C		Use the readlink() function properly
CERT C Secure Coding	STR03-C		Do not inadvertently truncate a null-terminated byte string
CERT C Secure Coding	STR32-C		Null-terminate byte strings as required

White Box Definitions

A weakness where the code path has:

1. end statement that passes a data item to a null-terminated string function
2. start statement that produces the improper null-terminated data item

Where "produces" is defined through the following scenarios:

1. data item never ended with null-terminator
2. null-terminator is re-written

Maintenance Notes

As currently described, this entry is more like a category than a weakness.

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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Causal Nature, Common Consequences, Description, Likelihood of Exploit, Maintenance Notes, Relationships, Other Notes, Relationship 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 Common Consequences		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Common Consequences, Other Notes, Potential Mitigations, White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description		

BACK TO TOP

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;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
    {
        total = op1 + op2;
    }
    else
```

```
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

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

Short Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()

{

	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

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

{

	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

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

{

	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

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

{

	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

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

{

	printf("%s", argv[1]); // Second parameter is not a formattable string

	return 0;
}
```

Improper Sanitization of Special Elements used in a Command ('Command Injection')

Weakness ID: 77 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended command when it is sent to a downstream component.

Extended Description

Command injection vulnerabilities typically occur when:

1. Data enters the application from an untrusted source.
2. The data is part of a string that is executed as a command by the application.
3. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Access Control	Command injection allows for the execution of arbitrary commands and code by the attacker.
Integrity	If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed.

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following simple program accepts a filename as a command line argument and displays the contents of the file back to the user. The program is installed setuid root because it is intended for use as a learning tool to allow system administrators in-training to inspect privileged system files without giving them the ability to modify them or damage the system.

Example Language: **C**

```
int main(char* argc, char** argv) {
char cmd[CMD_MAX] = "/usr/bin/cat ";
strcat(cmd, argv[1]);
system(cmd);
}
```

Because the program runs with root privileges, the call to system() also executes with root privileges. If a user specifies a standard filename, the call works as expected. However, if an attacker passes a string of the form ";rm -rf /", then the call to system() fails to execute cat due to a lack of arguments and then plows on to recursively delete the contents of the root partition.

Example 2

The following code is from an administrative web application designed to allow users to kick off a backup of an Oracle database using a batch-file wrapper around the rman utility and then run a cleanup.bat script to delete some temporary files. The script rmanDB.bat accepts a single command line parameter, which specifies what type of backup to perform. Because access to the database is restricted, the application runs the backup as a privileged user.

(Bad Code)

Example Language: **Java**

```
...
String btype = request.getParameter("backuptype");
String cmd = new String("cmd.exe /K \"
c:\\util\\rmanDB.bat "
+btype+
"&&c:\\utl\\cleanup.bat\"")
System.Runtime.getRuntime().exec(cmd);
...
```

The problem here is that the program does not do any validation on the backuptype parameter read from the user. Typically the Runtime.exec() function will not execute multiple commands, but in this case the program first runs the cmd.exe shell in order to run multiple commands with a single call to Runtime.exec(). Once the shell is invoked, it will happily execute multiple commands separated by two ampersands. If an attacker passes a string of the form "& del c:\\dbms*.*", then the application will execute this command along with the others specified by the program. Because of the nature of the application, it runs with the privileges necessary to interact with the database, which means whatever command the attacker injects will run with those privileges as well.

Example 3

The following code from a system utility uses the system property APPHOME to determine the directory in which it is installed and then executes an initialization script based on a relative path from the specified directory.

(Bad Code)

Example Language: **Java**

```
...
String home = System.getProperty("APPHOME");
String cmd = home + INITCMD;
java.lang.Runtime.getRuntime().exec(cmd);
...
```

The code above allows an attacker to execute arbitrary commands with the elevated privilege of the application by modifying the system property APPHOME to point to a different path containing a malicious version of INITCMD. Because the program does not validate the value read from the environment, if an attacker can control the value of the system property APPHOME, then they can fool the application into running malicious code and take control of the system.

Example 4

The following code is from a web application that allows users access to an interface through which they can update their password on the system. Part of the process for updating passwords in certain network environments is to run a make command in the /var/yp directory, the code for which is shown below.

(Bad Code)

Example Language: **Java**

```
...
System.Runtime.getRuntime().exec("make");
...
```

The problem here is that the program does not specify an absolute path for make and

fails to clean its environment prior to executing the call to Runtime.exec(). If an attacker can modify the $PATH variable to point to a malicious binary called make and cause the program to be executed in their environment, then the malicious binary will be loaded instead of the one intended. Because of the nature of the application, it runs with the privileges necessary to perform system operations, which means the attacker's make will now be run with these privileges, possibly giving the attacker complete control of the system.

Example 5

The following code is a wrapper around the UNIX command cat which prints the contents of a file to standard out. It is also injectable:

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {

char cat[] = "cat ";
char *command;
size_t commandLength;

commandLength = strlen(cat) + strlen(argv[1]) + 1;
command = (char *) malloc(commandLength);
strncpy(command, cat, commandLength);
strncat(command, argv[1], (commandLength - strlen(cat)) );

system(command);
return (0);
}
```

Used normally, the output is simply the contents of the file requested:

```
$ ./catWrapper Story.txt
When last we left our heroes...
```

However, if we add a semicolon and another command to the end of this line, the command is executed by catWrapper with no complaint:

(Attack)

```
$ ./catWrapper Story.txt; ls
When last we left our heroes...
Story.txt
SensitiveFile.txt
PrivateData.db
a.out*
```

If catWrapper had been set to have a higher privilege level than the standard user, arbitrary commands could be executed with that higher privilege.

Potential Mitigations

Phase: Architecture and Design

If at all possible, use library calls rather than external processes to recreate the desired functionality

Phase: Implementation

If possible, ensure that all external commands called from the program are statically created.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

Run time: Run time policy enforcement may be used in a white-list fashion to prevent use of any non-sanctioned commands.

Assign permissions to the software system that prevents the user from accessing/opening privileged files.

Other Notes

Command injection is a common problem with wrapper programs.

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	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	74	Failure to Sanitize Data into a Different Plane ('Injection')	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	713	OWASP Top Ten 2007 Category A2 - Injection Flaws	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711
ChildOf	Category	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ParentOf	Weakness Base	78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	88	Argument Injection or Modification	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	90	Failure to Sanitize Data into LDAP Queries ('LDAP Injection')	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	624	Executable Regular Expression Error	**Development Concepts (primary)699 Research Concepts (primary)1000**

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Command Injection
CLASP			Command injection

OWASP Top Ten 2007	A2	CWE More Specific	Injection Flaws
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A6	CWE More Specific	Injection Flaws

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
15	Command Delimiters	
23	File System Function Injection, Content Based	
43	Exploiting Multiple Input Interpretation Layers	
75	Manipulating Writeable Configuration Files	
6	Argument Injection	
11	Cause Web Server Misclassification	
76	Manipulating Input to File System Calls	

References

G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. February 2004.

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 Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Name		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Other Notes, Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Command Injection
2009-05-27	Failure to Sanitize Data into a Control Plane (aka 'Command Injection')
2009-07-27	Failure to Sanitize Data into a Control Plane ('Command Injection')

BACK TO TOP

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;
}
```

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.
An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

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 After Free

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
//..
```

Use of Uninitialized Pointer

Risk

What might happen

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

Cause

How does it happen

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

General Recommendations

How to avoid it

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

Source Code Examples

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

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

Cause

How does it happen

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

General Recommendations

How to avoid it

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

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Wrong Memory Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
```

```
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Uncontrolled Recursion

Weakness ID: 674 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product does not properly control the amount of recursion that takes place, which consumes excessive resources, such as allocated memory or the program stack.

Alternate Terms

Stack Exhaustion

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Availability	Resources including CPU, memory, and stack memory could be rapidly consumed or exhausted, eventually leading to an exit or crash.
Confidentiality	In some cases, an application's interpreter might kill a process or thread that appears to be consuming too much resources, such as with PHP's memory_limit setting. When the interpreter kills the process/thread, it might report an error containing detailed information such as the application's installation path.

Observed Examples

Reference	Description
CVE-2007-1285	Deeply nested arrays trigger stack exhaustion.
CVE-2007-3409	Self-referencing pointers create infinite loop and resultant stack exhaustion.

Potential Mitigations

Limit the number of recursive calls to a reasonable number.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Development Concepts (primary)699**
ChildOf	Weakness Class	691	Insufficient Control Flow Management	**Research Concepts (primary)1000**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**

Affected Resources

- CPU

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
82	Violating Implicit Assumptions Regarding XML Content (aka XML Denial of Service (XDoS))	
99	XML Parser Attack	

Content History

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 Common Consequences, Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

BACK TO TOP

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

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

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in

the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

BACK TO TOP

Leaving Temporary Files

Risk

What might happen

Applications often create temporary files containing sensitive business data or personal information, in order to handle the file generation process in several steps, or even as the output of an automatic process. These files, if left exposed on disk for an indeterminate period of time, could leak the secret data to unauthorized users.

Cause

How does it happen

It is very common for applications to use temporary files, as intermediate storage and to aid with processing large amounts of data or long-running calculations. Applications require such files so frequently that most operating systems allocate a dedicated area for temporary files, such as a TEMP directory, and several different mechanisms for creating them exist in most platforms. However, by default these temporary files are not deleted automatically, and will remain on disk indefinitely. If the program does not explicitly and proactively delete the temporary files when it is finished processing them, they might be accessbile to other users of the computer.

General Recommendations

How to avoid it

- Always explicitly delete any temporary file created. Ensure temp file deletion will occur by wrapping it in a `finally { }` block, or call `File.deleteOnExit()` to ensure eventual deletion.
- Additionally, to ensure that all temporary files will eventually be deleted, consider implementing additional functionality that will periodically scrape and delete all unused, existing temporary files.
- Ensure all existing file handles or references are closed before attempting deletion.

Source Code Examples

Java

Leaving Temporary Report File

```
private byte[] generateData(int key) {
      File tempFile = File.createTempFile(TEMP_PREFIX, ".txt");

      FileOutputStream writer = new FileOutputStream(tempFile);
      ReportGenerator.writeHugeReportToFileStream(writer, key);

      FileInputStream reader = new FileInputStream(tempFile);
      int length = reader.available();
      if (length > 0) {
            byte[] reportData = new byte[length];
            reader.read(reportData);

            return reportData;
    }
      else {
            return null;
    }
```

```
}
```

Cleaning Up Temporary Report File

```
private byte[] generateData(int key) {
      byte[] reportData = null;
      File tempFile = null;
      FileOutputStream writer = null;
      FileInputStream reader = null;

      try {
      tempFile = File.createTempFile(TEMP_PREFIX, ".txt");

      writer = new FileOutputStream(tempFile);
      ReportGenerator.writeHugeReportToFileStream(writer, key);

      reader = new FileInputStream(tempFile);
      int length = reader.available();
      if (length > 0) {
               reportData = new byte[length];
          reader.read(reportData);
      }
    }
      catch (IOException e) {
             handleError(e);
    }
      finally {
             if (reader != null) {
             try {
                    reader.close();
             }
                    catch (IOException e) {
                           handleError(e);
             }
        }

             if (writer != null) {
             try {
                    writer.close();
             }
             catch (IOException e) {
                 handleError(e);
             }
        }

             if (tempFile != null) {
             try {
             tempFile.delete();
             }
             catch (IOException e) {
                 handleError(e);
             }
        }
    }
      return reportData;
}
```

Improper Access Control (Authorization)

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

Description

Description Summary

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

Extended Description

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

Alternate Terms

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

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

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

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

Common Consequences

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

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

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

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

Effectiveness: Limited

Automated Dynamic Analysis

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

Manual Analysis

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

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

Effectiveness: Moderate

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

Demonstrative Examples

Example 1

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

(Bad Code)

Example Language: **Perl**

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

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

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

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

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

Observed Examples

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

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

Potential Mitigations

Phase: Architecture and Design

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

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

Phase: Architecture and Design

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

Phase: Architecture and Design

Strategy: Libraries or Frameworks

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

easier to avoid.

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

Phase: Architecture and Design

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

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

Phases: System Configuration; Installation

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

Relationships

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

Taxonomy Mappings

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

Related Attack Patterns

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

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

References

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

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

Content History

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

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

Potential Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
```

```
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

NULL Pointer Dereference

Risk

What might happen

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

Cause

How does it happen

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

General Recommendations

How to avoid it

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

Source Code Examples

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

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--;
           }
        }
    }
```

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

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

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