471920 Scan Report

Project Name	471920
Scan Start	Sunday, December 13, 2015 8:12:56 PM
Preset	Default
Scan Time	00h:14m:03s
Lines Of Code Scanned	177423
Files Scanned	1469
Report Creation Time	Monday, December 14, 2015 2:37:39 AM
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445
Team	11389
Checkmarx Version	7.2.3
Scan Type	Full
Source Origin	LocalPath
Density	2/1000 (Vulnerabilities/LOC)
Access	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: Confirmed, Not Exploitable, To Verify, Urgent

Excluded: None

Assigned to

Included: All

Categories

Included: Uncategorized, Must audit, Check, Optional

Excluded: None

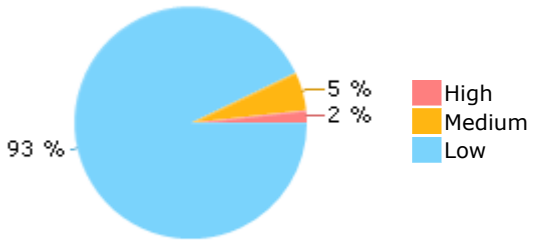
Results Limit

A limit was not defined

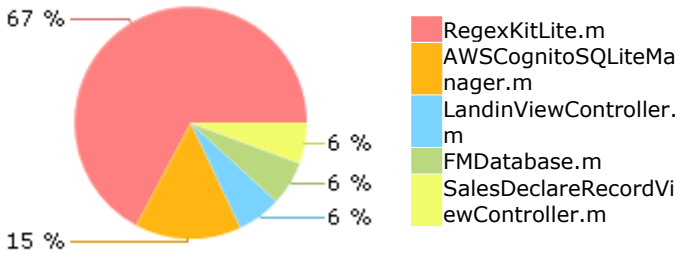
Selected Queries

Selected queries are listed in Result Summary

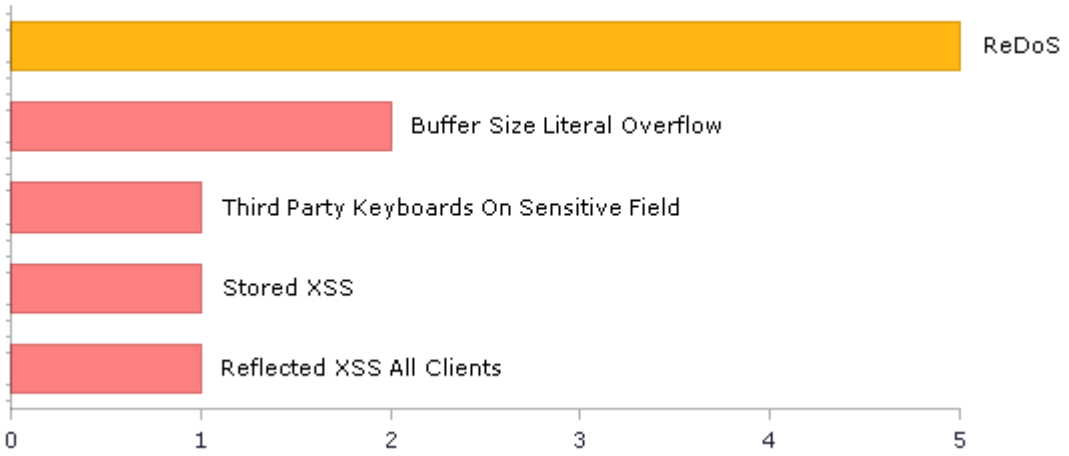
Result Summary



Most Vulnerable Files



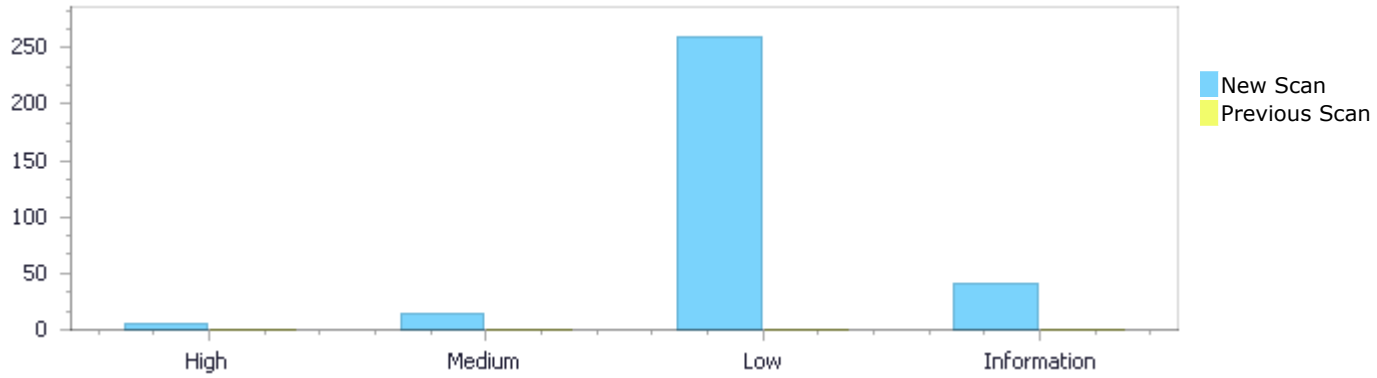
Top 5 Vulnerabilities



Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	5	15	260	41	321
Recurrent Issues	0	0	0	0	0
Total	5	15	260	41	321
Fixed Issues	0	0	0	0	0



Results Distribution By State

	High	Medium	Low	Information	Total
To Verify	5	15	260	41	321
Not Exploitable	0	0	0	0	0
Confirmed	0	0	0	0	0
Urgent	0	0	0	0	0
Total	5	15	260	41	321

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Size Literal Overflow	2	High
Reflected XSS All Clients	1	High
Stored XSS	1	High
Third Party Keyboards On Sensitive Field	1	High
ReDoS	5	Medium
Insecure Data Storage	2	Medium
Missing Encryption of Sensitive Data	2	Medium
Path Manipulation	2	Medium
Cut And Paste Leakage	1	Medium
Improper Certificate Validation	1	Medium
Screen Caching	1	Medium
Side Channel Data Leakage	1	Medium
Buffer Size Literal Condition	132	Low
Jailbrake File Referenced By Name	48	Low

Unscrubbed Secret	37	Low
Unchecked CString Convertion	17	Low
Use of Broken or Risky Cryptographic Algorithm	7	Low
Functions Apple Recommends To Avoid	5	Low
Improper Resource Shutdown or Release	4	Low
Jailbreak Unchecked File Operation Result Code	3	Low
Use of Hardcoded Password	3	Low
Memory Leak	2	Low
Unchecked Return Value	2	Low
Dynamic SQL Queries	41	Information

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
/intelRetailstore/intelRetailstore/LandinViewController.m	4
/intelRetailstore/RegexKitLite/RegexKitLite.m	2
/intelRetailstore/intelRetailstore/LandinViewController.h	2
/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m	2
/intelRetailstore/intelRetailstore/reward/OrderDetailViewController.h	2
/intelRetailstore/AFNetworking/AFNetworking/AFHTTPRequestOperation.m	1
/intelRetailstore/AFNetworking/UIKit+AFNetworking/UIWebView+AFNetworking.m	1
/intelRetailstore/CustomView/TermsView.m	1
/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSIdentityProvider.m	1
/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m	1

Scan Results Details

Buffer Size Literal Overflow

Query Path:
Objc\Cx\Apple Secure Coding Guide\Buffer Size Literal Overflow Version:0

Description

Buffer Size Literal Overflow\Path 21:

Severity	High
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=21
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.mspecifies the size of a buffer. At line 162 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSIdentityProvider.m this number literal is used in a conditional statement with <= operator instead of <. This may cause a buffer overflow.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSIdentityProvider.m
Line	377	164
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSIdentityProvider.m

Method return [[[BFTask taskWithResult:nil] continueWithExecutor:self.executor withBlock:^id(BFTask *task) {

```
....
164.              if (self.count <= 1) {
```

Buffer Size Literal Overflow\Path 22:

Severity	High

Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=22
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.mspecifies the size of a buffer. At line 553 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m this number literal is used in a conditional statement with <= operator instead of <. This may cause a buffer overflow.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m
Line	377	555
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m

Method return [[[BFTask taskWithResult:nil] continueWithExecutor:self.refreshExecutor withSuccessBlock:^id(BFTask *task) {

```
....
555.          if (self.count <= 1) {
```

Reflected XSS All Clients

Query Path:
Objc\Cx\ObjectiveC High Risk\Reflected XSS All Clients Version:0

Description

Reflected XSS All Clients\Path 1:

Severity	High
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=1
Status	New

Method AFHTTPRequestOperation at line 60 of /intelRetailstore/AFNetworking/AFNetworking/AFHTTPRequestOperation.m gets user input for

the _response element. This element’s value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method setCompletionBlockWithSuccess:^ at line 132 of /intelRetailstore/AFNetworking/UIKit+AFNetworking/UIWebView+AFNetworking.m. This may enable a Cross-Site-Scripting attack.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFHTTPRequestOperation.m	/intelRetailstore/AFNetworking/UIKit+AFNetworking/UIWebView+AFNetworking.m
Line	60	138
Object	_response	data

Code Snippet

File Name /intelRetailstore/AFNetworking/AFNetworking/AFHTTPRequestOperation.m

Method @implementation AFHTTPRequestOperation

```
....
60.  @implementation AFHTTPRequestOperation
```

File Name /intelRetailstore/AFNetworking/UIKit+AFNetworking/UIWebView+AFNetworking.m

Method [self.af_HTTPRequestOperation setCompletionBlockWithSuccess:^(AFHTTPRequestOperation *operation, id __unused responseObject) {

```
....
138.          [strongSelf loadData:data MIMEType:(MIMEType ?:
[operation.response MIMEType]) textEncodingName:(textEncodingName ?:
[operation.response textEncodingName]) baseURL:[operation.response
URL]];
```

Stored XSS

Query Path:

Objc\Cx\ObjectiveC High Risk\Stored XSS Version:0

Description

Stored XSS\Path 2:

Severity	High
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=2
Status	New

Method - at line 12 of /intelRetailstore/CustomView/TermsView.m gets data from the database, for the stringWithContentsOfFile:encoding:error: element. This element’s value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method - at line 12 of /intelRetailstore/CustomView/TermsView.m. This may enable a Stored Cross-Site-Scripting attack.

	Source	Destination
File	/intelRetailstore/CustomView/TermsView.m	/intelRetailstore/CustomView/TermsView.m

Line	31	40
Object	stringWithContentsOfFile:encoding:error:	intelTermContents

Code Snippet
File Name /intelRetailstore/CustomView/TermsView.m
Method - (id)initWithFrame:(CGRect)frame{

```
....
31.          NSString    *intelTermContents = [NSString
stringWithContentsOfFile:
....
40.          [intelWebView loadHTMLString:intelTermContents
baseURL:[NSURL fileURLWithPath:[[NSBundle mainBundle]bundlePath]]];
```

Third Party Keyboards On Sensitive Field

Query Path:
Objc\Cx\ObjectiveC High Risk\Third Party Keyboards On Sensitive Field Version:1

Description

Third Party Keyboards On Sensitive Field\Path 23:

Severity	High
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=23
Status	New

The passwordTextField at line 15 of /intelRetailstore/intelRetailstore/LandinViewController.h contains sensitive data, and is not protected from third party keyboards by either: 1) Setting secureTextEntry=YES, -Or- 2) Disabling third party keyboards application wide.

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.h	/intelRetailstore/intelRetailstore/LandinViewController.h
Line	15	15
Object	passwordTextField	passwordTextField

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.h
Method @property (weak, nonatomic) IBOutlet UITextField *passwordTextField;

```
....
15.  @property (weak, nonatomic) IBOutlet UITextField
*passwordTextField;
```

ReDoS

Query Path:
Objc\Cx\ObjectiveC Medium Threat\ReDoS Version:0

Description

ReDoS\Path 6:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&pr

	ojectid=10445&pathid=6
Status	New

The input text at line 719 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m is used to create a regular expression pattern at line 759 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m. An evil pattern may be injected into a regex matching engine.

	Source	Destination
File	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	723	762
Object	text	stringByReplacingMatchesInString:options:range:withTemplate:

Code Snippet

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method - (void)textViewDidChange:(UITextView *)textView{

```
....
723.      NSString *toBeString = textView.text;
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method - (NSString *)disable_emoji:(NSString *)text

```
....
762.      NSString *modifiedString = [regex
stringByReplacingMatchesInString:text
```

ReDoS\Path 7:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=7
Status	New

The input text at line 789 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m is used to create a regular expression pattern at line 759 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m. An evil pattern may be injected into a regex matching engine.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Consulta	/intelRetailstore/intelRetailstore/Consulta

	tionWithFeedback/AddQuestionViewController.m	tionWithFeedback/AddQuestionViewController.m
Line	792	762
Object	text	stringByReplacingMatchesInString:options:range:withTemplate:

Code Snippet
File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Method -(void)limitLength:(id)obj{

```
....
792.      NSString *toBeString = textField.text;
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Method - (NSString *)disable_emoji:(NSString *)text

```
....
762.      NSString *modifiedString = [regex
stringByReplacingMatchesInString:text
```

ReDoS\Path 8:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=8
Status	New

The input text at line 308 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/CheckAnswerViewController.m is used to create a regular expression pattern at line 344 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/CheckAnswerViewController.m. An evil pattern may be injected into a regex matching engine.

	Source	Destination
File	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/CheckAnswerViewController.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/CheckAnswerViewController.m
Line	309	347
Object	text	stringByReplacingMatchesInString:options:range:withTemplate:

Code Snippet
File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/CheckAnswerViewController.m
Method - (void)textViewDidChange:(UITextView *)textView{

```
....
309.      NSString *toBeString = textView.text;
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/CheckAnswerViewController.m

Method - (NSString *)disable_emoji:(NSString *)text

```
....
347.      NSString *modifiedString = [regex
stringByReplacingMatchesInString:text
```

ReDoS\Path 9:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=9
Status	New

The input text at line 494 of /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m is used to create a regular expression pattern at line 523 of /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m. An evil pattern may be injected into a regex matching engine.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m
Line	498	526
Object	text	stringByReplacingMatchesInString:options:range:withTemplate:

Code Snippet

File Name /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m

Method - (void)textFieldTextDidChanged:(id)sender

```
....
498.      textField.text = [self disable_emoji:textField.text];
```

File Name /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m

Method - (NSString *)disable_emoji:(NSString *)text

```
....
526.      NSString *modifiedString = [regex
stringByReplacingMatchesInString:text
```

ReDoS\Path 10:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=10
Status	New

The input text at line 717 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m is used to create a regular expression pattern at line 751 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m. An evil pattern may be injected into a regex matching engine.

	Source	Destination
File	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Line	718	754
Object	text	stringByReplacingMatchesInString:options:range:withTemplate:

Code Snippet

File Name /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m

Method - (void)textViewDidChange:(UITextView *)textView{

```
....
718.      NSString *toBeString = textView.text;
```

File Name /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m

Method - (NSString *)disable_emoji:(NSString *)text

```
....
754.      NSString *modifiedString = [regex
stringByReplacingMatchesInString:text
```

Insecure Data Storage

Query Path:

Objc\Cx\ObjectiveC Medium Threat\Insecure Data Storage Version:0

Description

Insecure Data Storage\Path 4:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=4
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	383

Object	_passwordTextField	text

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

File Name /intelRetailstore/intelRetailstore/LandinViewController.m

Method [operationManager POST:landinUrlStr parameters:parameters success:^(AFHTTPRequestOperation *operation, id responseObject) {

```
....
383.                  [userDefaults
setObject:self.passwordTextField.text forKey:K_USERDEFAULTS_PASS];
```

Insecure Data Storage\Path 5:

Severity Medium
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=5
Status New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	389
Object	_passwordTextField	text

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

File Name /intelRetailstore/intelRetailstore/LandinViewController.m

Method [operationManager POST:landinUrlStr parameters:parameters success:^(AFHTTPRequestOperation *operation, id responseObject) {

```
....
389.              [userDefaults setObject:self.passwordTextField.text
forKey:K_USERDEFAULTS_LOCALPASS];
```

Missing Encryption of Sensitive Data

Query Path:
Objc\Cx\ObjectiveC Medium Threat\Missing Encryption of Sensitive Data Version:0

Description

Missing Encryption of Sensitive Data\Path 13:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=13
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	383
Object	_passwordTextField	text

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

File Name /intelRetailstore/intelRetailstore/LandinViewController.m

Method [operationManager POST:landinUrlStr parameters:parameters success:^(AFHTTPRequestOperation *operation, id responseObject) {

```
....
383.                    [userDefaults
setObject:self.passwordTextField.text forKey:K_USERDEFAULTS_PASS];
```

Missing Encryption of Sensitive Data\Path 14:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=14
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	389
Object	_passwordTextField	text

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

File Name /intelRetailstore/intelRetailstore/LandinViewController.m

Method [operationManager POST:landinUrlStr parameters:parameters success:^(AFHTTPRequestOperation *operation, id responseObject) {

```
....
389.              [userDefaults setObject:self.passwordTextField.text
forKey:K_USERDEFAULTS_LOCALPASS];
```

Path Manipulation

Query Path:
Objc\Cx\Apple Secure Coding Guide\Path Manipulation Version:0

Description

Path Manipulation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=19
Status	New

	Source	Destination
File	/intelRetailstore/SDWebImage/SDImageCache.m	/intelRetailstore/SDWebImage/SDImageCache.m
Line	250	135
Object	UIImage	createFileAtPath:contents:attributes:

Code Snippet

File Name /intelRetailstore/SDWebImage/SDImageCache.m

Method - (UIImage *)imageFromKey:(NSString *)key fromDisk:(BOOL)fromDisk

```
....
250.          image = [[[UIImage alloc] initWithContentsOfFile:[self
cachePathForKey:key]] autorelease];
```

File Name /intelRetailstore/SDWebImage/SDImageCache.m

Method - (void)storeKeyWithDataToDisk:(NSArray *)keyAndData

```
....
135.              [fileManager createFileAtPath:[self
cachePathForKey:key] contents:UIImageJPEGRepresentation(image,
(CGFloat)1.0) attributes:nil];
```

Path Manipulation\Path 20:

Severity	Medium
Result State	To Verify

Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=20
Status	New

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	204	206
Object	processInfo	moveItemAtURL:toURL:error:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method +(BOOL)moveItemAtURLToTrash:(NSURL *)itemURL

```
....
204.      NSString *uniqueString = [[NSProcessInfo processInfo]
globallyUniqueString];
....
206.      BOOL moved = [[NSFileManager defaultManager]
moveItemAtURL:itemURL toURL:uniqueTrashURL error:&error];
```

Cut And Paste Leakage

Query Path:
Objc\Cx\ObjectiveC Medium Threat\Cut And Paste Leakage Version:1

Description

Cut And Paste Leakage\Path 3:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=3
Status	New

The UI element passwordTextField at line 15 of /intelRetailstore/intelRetailstore/LandinViewController.h displays sensitive data on screen. Copying of this sensitive data to a paste board is not prevented by any means.

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.h	/intelRetailstore/intelRetailstore/LandinViewController.h
Line	15	15
Object	passwordTextField	passwordTextField

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.h
Method @property (weak, nonatomic) IBOutlet UITextField *passwordTextField;

```
....
15.  @property (weak, nonatomic) IBOutlet UITextField
*passwordTextField;
```

Improper Certificate Validation

Query Path:
Objc\Cx\ObjectiveC Medium Threat\Improper Certificate Validation Version:0
Description
Improper Certificate Validation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=15
Status	New

The UI element credentialForTrust: at line 86 of /intelRetailstore/intelRetailstore/Performance/integralDetailViewController.m disables the validation of the TLS/SSL server certificates. The inevitable outcome is that a 'man in the middle' attack is not prevented.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Performance/integralDetailViewController.m	/intelRetailstore/intelRetailstore/Performance/integralDetailViewController.m
Line	94	96
Object	credentialForTrust:	cre

Code Snippet
File Name /intelRetailstore/intelRetailstore/Performance/integralDetailViewController.m
Method - (void)connection:(NSURLConnection *)connection willSendRequestForAuthenticationChallenge:(NSURLAuthenticationChallenge *)challenge

```
....
94.          NSURLCredential* cre = [NSURLCredential
credentialForTrust:challenge.protectionSpace.serverTrust];
....
96.          [challenge.sender useCredential:cre
forAuthenticationChallenge:challenge];
```

Screen Caching

Query Path:
Objc\Cx\ObjectiveC Medium Threat\Screen Caching Version:0
Description
Screen Caching\Path 17:

Severity	Medium
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=17
Status	New

The UI element userAccount at line 15 of /intelRetailstore/intelRetailstore/reward/OrderDetailViewController.h displays sensitive data on screen. Background screen caching of this sensitive information is not prevented by any means.

	Source	Destination
File	/intelRetailstore/intelRetailstore/reward/	/intelRetailstore/intelRetailstore/reward/

	OrderDetailViewController.h	OrderDetailViewController.h
Line	15	15
Object	userAccount	userAccount

Code Snippet
File Name /intelRetailstore/intelRetailstore/reward/OrderDetailViewController.h
Method @property (weak, nonatomic) IBOutlet UILabel *userAccount;

```
....
15.  @property (weak, nonatomic) IBOutlet UILabel *userAccount;
```

Side Channel Data Leakage

Query Path:
Objc\Cx\ObjectiveC Medium Threat\Side Channel Data Leakage Version:0

Description

Side Channel Data Leakage\Path 25:

Severity Medium
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=25
Status New

	Source	Destination
File	/intelRetailstore/intelRetailstore/reward/OrderDetailViewController.h	/intelRetailstore/intelRetailstore/reward/OrderDetailViewController.h
Line	15	15
Object	userAccount	userAccount

Code Snippet
File Name /intelRetailstore/intelRetailstore/reward/OrderDetailViewController.h
Method @property (weak, nonatomic) IBOutlet UILabel *userAccount;

```
....
15.  @property (weak, nonatomic) IBOutlet UILabel *userAccount;
```

Buffer Size Literal Condition

Query Path:
Objc\Cx\Apple Secure Coding Guide\Buffer Size Literal Condition Version:0

Description

Buffer Size Literal Condition\Path 155:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=155
Status New

The number literal 4 at line 28 of /intelRetailstore/NSData+Base64.m specifies the size of a buffer. At line 28 of /intelRetailstore/NSData+Base64.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/NSData+Base64.m	/intelRetailstore/NSData+Base64.m
Line	35	75
Object	4	4

Code Snippet
File Name /intelRetailstore/NSData+Base64.m
Method - (id) initWithBase64EncodedString:(NSString *) string {

```
....
35.         unsigned char inbuf[3], outbuf[4];
....
75.                         if( ixinbuf == 4 ) {
```

Buffer Size Literal Condition\Path 156:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=156
Status	New

The number literal 3 at line 94 of /intelRetailstore/NSData+Base64.m specifies the size of a buffer. At line 94 of /intelRetailstore/NSData+Base64.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/NSData+Base64.m	/intelRetailstore/NSData+Base64.m
Line	100	109
Object	3	3

Code Snippet
File Name /intelRetailstore/NSData+Base64.m
Method - (NSString *) base64EncodingWithLineLength:(unsigned int) lineLength {

```
....
100.        unsigned char inbuf[3], outbuf[4];
....
109.              for( i = 0; i < 3; i++ ) {
```

Buffer Size Literal Condition\Path 157:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=157
Status	New

The number literal 4 at line 94 of /intelRetailstore/NSData+Base64.m specifies the size of a buffer. At line 94 of /intelRetailstore/NSData+Base64.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/NSData+Base64.m	/intelRetailstore/NSData+Base64.m
Line	100	133
Object	4	4

Code Snippet
File Name /intelRetailstore/NSData+Base64.m
Method - (NSString *) base64EncodingWithLineLength:(unsigned int) lineLength {

```
....
100.        unsigned char inbuf[3], outbuf[4];
....
133.              for( i = ctcopy; i < 4; i++ )
```

Buffer Size Literal Condition\Path 158:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=158
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 74 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionPicDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionPicDetailViewController.m
Line	377	76
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionPicDetailViewController.m
Method	- (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex

```
....
76.      if (buttonIndex ==1) {
```

Buffer Size Literal Condition\Path 159:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=159
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 79 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/OnlineQuestionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/OnlineQuestionViewController.m
Line	377	82
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/OnlineQuestionViewController.m
Method	-(void)addQuestion{

```
....
82.      if ([StoreDataArray sharedInstance].storeDataArray.count>1) {
```

Buffer Size Literal Condition\Path 160:

Severity	Low
Result State	To Verify

Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=160
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 166 of /intelRetailstore/intelRetailstore/Declaration/PreviewViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/PreviewViewController.m
Line	377	167
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/PreviewViewController.m

Method - (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex{

```
....
167.      if (buttonIndex == 1) {
```

Buffer Size Literal Condition\Path 161:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=161
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 213 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewContr

		oller.m
Line	377	222
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m
Method	- (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
222.      if (_selectArray.count<1) {
```

Buffer Size Literal Condition\Path 162:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=162
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 251 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m
Line	377	253
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m
Method	- (IBAction)batchModifyButtonClick:(id)sender {

```
....
253.      if (_selectArray.count<1) {
```

Buffer Size Literal Condition\Path 163:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=163
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 319 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m
Line	377	321
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m
Method	- (IBAction)selectAllButtonClick:(id)sender {

```
....
321.      if (_salesDeclareRecordArray.count<1) {
```

Buffer Size Literal Condition\Path 164:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=164
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 150 of /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m
Line	377	173
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m

Method - (IBAction)submitButtonClick:(id)sender {

```
....
173.      if (_modelTextField.text.length<1) {
```

Buffer Size Literal Condition\Path 165:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=165
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 65 of /intelRetailstore/intelRetailstore/EnterViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/EnterViewController.m
Line	377	114
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/EnterViewController.m

Method - (void)setScrollView{

```
....
114.      if (_imageArray.count>1) {
```

Buffer Size Literal Condition\Path 166:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=166
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 148 of /intelRetailstore/intelRetailstore/EnterViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/EnterViewController.m
Line	377	171
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/EnterViewController.m
Method	- (void)enter:(UIButton *)sender{

```
....
171.      if ([StoreDataArray sharedInstance].storeDataArray.count>1) {
```

Buffer Size Literal Condition\Path 167:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=167
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 28 of /intelRetailstore/intelRetailstore/IREP/IREPTrainCollectionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/IREPTrainCollectionViewController.m
Line	377	42
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/IREP/IREPTrainCollectionViewController.m
Method	- (void)viewDidLoad {

```
....
42.      if ([StoreDataArray sharedInstance].storeDataArray.count==1) {
```

Buffer Size Literal Condition\Path 168:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=168
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 262 of /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m
Line	377	269
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
269.      if (onlineTrainData.ifsign.integerValue == 1) {
```

Buffer Size Literal Condition\Path 169:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=169
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 502 of /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m
Line	377	506
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m

Method - (CGFloat)tableView:(UITableView *)tableView heightForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
506.      if (onlineTrainData.ifsign.integerValue == 1) {
```

Buffer Size Literal Condition\Path 170:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=170
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 82 of /intelRetailstore/intelRetailstore/Main/ApplicationCardDetailsViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/ApplicationCardDetailsViewController.m
Line	377	83
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/ApplicationCardDetailsViewController.m

Method - (CGFloat)tableView:(UITableView *)tableView heightForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
83.      if (indexPath.row == 1) {
```

Buffer Size Literal Condition\Path 171:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=171
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 124 of /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Line	377	129
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m

Method	- (void)confirmButtonClick:(id)sender {

```
....
129.      if (self.oldPassTextFiled.text.length<1) {
```

Buffer Size Literal Condition\Path 172:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=172
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 277 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Line	377	287
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Method	- (void)setScrollView{

```
....
287.      if (scrollViewPage == 1) {
```

Buffer Size Literal Condition\Path 173:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=173
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 647 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Line	377	660
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/MainViewController.m

Method - (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
660.      if (information.rec_sts_id.integerValue == 1) {
```

Buffer Size Literal Condition\Path 174:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=174
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 72 of /intelRetailstore/intelRetailstore/PasswordProtectionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Line	377	73
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Method	- (IBAction)enterButtonClick:(id)sender {

```
....
73.      if (self.passwordTextFiled.text.length<1) {
```

Buffer Size Literal Condition\Path 175:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=175
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 112 of /intelRetailstore/intelRetailstore/PasswordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/PasswordViewController.m
Line	377	117
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/PasswordViewController.m
Method	- (IBAction)getPassword:(id)sender {

```
....
117.      if (self.numberPhoneTextFiled.text.length<1) {
```

Buffer Size Literal Condition\Path 176:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=176
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 74 of /intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m
Line	377	91
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m

Method -(void)createImageView{

```
....
91.      if (self.picArray.count > 1) {
```

Buffer Size Literal Condition\Path 177:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=177
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 95 of

/intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m
Line	377	105
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m

Method -(void)removeImageView{

```
....
105.      if (self.picArray.count == 1) {
```

Buffer Size Literal Condition\Path 178:

Severity Low

Result State To Verify

Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=178

Status New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 80 of /intelRetailstore/intelRetailstore/StorefrontPicture/StorefrontPictureViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StorefrontPicture/StorefrontPictureViewController.m
Line	377	82
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/StorefrontPicture/StorefrontPictureViewController.m
Method	- (void)backButtonClick:(UIButton *)sender{

```
....
82.      if ([StoreDataArray sharedInstance].storeDataArray.count>1) {
```

Buffer Size Literal Condition\Path 179:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=179
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 74 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Line	377	171
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Method	-(void)initWithScrollView{

```
....
171.      if(_totalQuestionsNum==1){
```

Buffer Size Literal Condition\Path 180:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=180
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 202 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Line	377	204
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m

Method - (void)previousProblemButtonClick:(UIButton *)sender{

```
....
204.      if (_currentExam == 1) {
```

Buffer Size Literal Condition\Path 181:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=181
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 553 of

/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m
Line	377	555
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m

Method return [[[BFTask taskWithResult:nil] continueWithExecutor:self.refreshExecutor withSuccessBlock:^id(BFTask *task) {

```
....
555.          if (self.count <= 1) {
```

Buffer Size Literal Condition\Path 182:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=182
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 162 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSIdentityProvider.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSIdentityProvider.m
Line	377	164
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSIdentityProvider.m
Method	return [[[BFTask taskWithResult:nil] continueWithExecutor:self.executor withBlock:^id(BFTask *task) {

```
....
164.              if (self.count <= 1) {
```

Buffer Size Literal Condition\Path 183:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=183
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 59 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/util/AWSMobileAnalyticsStringUtils.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/util/AWSMobileAnalyticsStringUtils.m
Line	377	63
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/util/AWSMobileAnalyticsStringUtils.m
Method	+ (NSString *) trimString: (NSString *) origin_string

```
....
63.      if (target_length < 1)
```

Buffer Size Literal Condition\Path 184:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=184
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 1257 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSSerialization.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSSerialization.m
Line	377	1258
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSSerialization.m
Method	+ (NSString *)upperCaseFirstChar:(NSString *) inputString {

```
....
1258.      if ([inputString length] < 1) {
```

Buffer Size Literal Condition\Path 185:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=185
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 650 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	377	670
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method - (void)actionSheet:(UIActionSheet *)actionSheet clickedButtonAtIndex:(NSInteger)buttonIndex{

```
....
670.      }else if (buttonIndex == 1) {
```

Buffer Size Literal Condition\Path 186:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=186
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 137 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m

Line	377	153
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
153.      }else if (indexPath.row ==1){
```

Buffer Size Literal Condition\Path 187:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=187
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 168 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m
Line	377	196
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordChangeViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
196.      }else if (salesRecordData.rec_sts_id.integerValue == 1){
```

Buffer Size Literal Condition\Path 188:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=188
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 154 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordListViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordListViewController.m
Line	377	192
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordListViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
192.      }else if (salesRecordData.rec_sts_id.integerValue == 1){
```

Buffer Size Literal Condition\Path 189:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=189
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 64 of /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m
Line	377	73
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
73.      }else if (indexPath.section == 1){
```

Buffer Size Literal Condition\Path 190:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=190
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 97 of /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m
Line	377	100
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m

Method - (CGFloat)tableView:(UITableView *)tableView heightForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
100.      }else if (indexPath.section == 1){
```

Buffer Size Literal Condition\Path 191:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=191
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 264 of /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Line	377	278
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
278.      }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 192:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=192
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 464 of /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Line	377	469
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m

Method	- (CGFloat)tableView:(UITableView *)tableView heightForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
469.      }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 193:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=193
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 115 of /intelRetailstore/intelRetailstore/IREP/IREPTrainCollectionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/IREPTrainCollectionViewController.m
Line	377	134
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/IREP/IREPTrainCollectionViewController.m
Method	-(void)collectionView:(UICollectionView *)collectionView didSelectItemAtIndexPath:(NSIndexPath *)indexPath {

```
....
134.      }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 194:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=194
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 391 of /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m
Line	377	411
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m

Method - (void)examButtonClick:(ExamButton *)sender{

```
....
411.      }else if (sender.onlineTrainData.exam_times.integerValue ==
1){
```

Buffer Size Literal Condition\Path 195:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=195
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 57 of /intelRetailstore/intelRetailstore/Main/AboutIntelRetailStoreViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/AboutIntelRetailStoreViewController.m
Line	377	61
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/AboutIntelRetailStoreViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
61.      }else if(indexPath.row == 1){
```

Buffer Size Literal Condition\Path 196:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=196
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 71 of /intelRetailstore/intelRetailstore/Main/AboutIntelRetailStoreViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/AboutIntelRetailStoreViewController.m
Line	377	86
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/AboutIntelRetailStoreViewController.m
Method	- (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
86.      }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 197:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=197
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 52 of /intelRetailstore/intelRetailstore/Main/ApplicationsettingsViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/ApplicationsettingsViewController.m
Line	377	66
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/ApplicationsettingsViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
66.      }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 198:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=198

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 167 of /intelRetailstore/intelRetailstore/Main/ApplicationsettingsViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/ApplicationsettingsViewController.m
Line	377	171
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/ApplicationsettingsViewController.m

Method - (CGFloat)tableView:(UITableView *)tableView heightForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
171.      }else if(indexPath.row == 1){
```

Buffer Size Literal Condition\Path 199:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=199
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 95 of /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Line	377	103

Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
103.      }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 200:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=200
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 62 of /intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m
Line	377	94
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
94.      }else if (indexPath.section == 1){
```

Buffer Size Literal Condition\Path 201:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=201
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 600 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Line	377	605
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Method	- (void)actionSheet:(UIActionSheet *)actionSheet clickedButtonAtIndex:(NSInteger)buttonIndex{

```
....
605.      }else if (buttonIndex == 1){
```

Buffer Size Literal Condition\Path 202:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=202

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 107 of /intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m
Line	377	112
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m

Method - (void)actionSheet:(UIActionSheet *)actionSheet clickedButtonAtIndex:(NSInteger)buttonIndex{

```
....
112.      }else if (buttonIndex == 1){
```

Buffer Size Literal Condition\Path 203:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=203
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 58 of /intelRetailstore/intelRetailstore/StoreDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StoreDetailViewController.m
Line	377	61
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/StoreDetailViewController.m
Method	-(CGFloat)tableView:(UITableView *)tableView heightForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
61.      }else if(indexPath.row ==1){
```

Buffer Size Literal Condition\Path 204:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=204
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 62 of /intelRetailstore/intelRetailstore/StorefrontData/SalesmanDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StorefrontData/SalesmanDetailViewController.m
Line	377	79
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/StorefrontData/SalesmanDetailViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
79.      }else if(indexPath.row ==1){
```

Buffer Size Literal Condition\Path 205:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=205
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 152 of /intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m
Line	377	161
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m
Method	-(UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
161.      }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 206:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=206

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 99 of /intelRetailstore/intelRetailstore/StorefrontPicture/StorefrontPictureViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StorefrontPicture/StorefrontPictureViewController.m
Line	377	116
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/StorefrontPicture/StorefrontPictureViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
116.      }else if (indexPath.row ==1){
```

Buffer Size Literal Condition\Path 207:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=207
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 554 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m

Line	377	585
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Method - (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
585.      }else if (type == 1)
```

Buffer Size Literal Condition\Path 208:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=208
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 275 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m
Line	377	278
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m
Method	- (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex

```
....
278.          if (buttonIndex ==1) {
```

Buffer Size Literal Condition\Path 209:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=209
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 154 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordListViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordListViewController.m
Line	377	161
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordListViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
161.          if (salesRecordData.pcsr_nbr.length<1) {
```

Buffer Size Literal Condition\Path 210:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=210
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 265 of /intelRetailstore/intelRetailstore/IREP/IntoStoreTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/IntoStoreTrainViewController.m
Line	377	287
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/IntoStoreTrainViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
287.          if(intoStoreTrainData.ifpass.integerValue == 1){
```

Buffer Size Literal Condition\Path 211:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=211
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 262 of /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m
Line	377	280
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
280.          if (onlineTrainData.ifpass.integerValue == 1) {
```

Buffer Size Literal Condition\Path 212:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=212
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 124 of /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Line	377	144
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Method - (void)confirmButtonClick:(id)sender {

```
....
144.          if (self.nowPassTextFiled.text.length<1) {
```

Buffer Size Literal Condition\Path 213:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=213
Status New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 118 of /intelRetailstore/intelRetailstore/QuestionSurveyViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/QuestionSurveyViewController.m
Line	377	140
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/QuestionSurveyViewController.m

Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
140.          if (questionData.ishasanswer == 1) {
```

Buffer Size Literal Condition\Path 214:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=214
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 151 of /intelRetailstore/intelRetailstore/QuestionSurveyViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/QuestionSurveyViewController.m
Line	377	163
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/QuestionSurveyViewController.m
Method	- (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath

```
....
163.          if (questionData.ishasanswer == 1) {
```

Buffer Size Literal Condition\Path 215:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=215
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 335 of /intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m
Line	377	346
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/StorefrontPicture/PicDetailViewController.m

Method - (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex

```
....
346.          if (buttonIndex == 1) {
```

Buffer Size Literal Condition\Path 216:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=216
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 232 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	377	239

Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method - (CGFloat)tableView:(UITableView *)tableView heightForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
239.          }else if (indexPath.row ==1){
```

Buffer Size Literal Condition\Path 217:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=217
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 256 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	377	288
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
288.          }else if (indexPath.row ==1){
```

Buffer Size Literal Condition\Path 218:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=218
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 275 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m
Line	377	345
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/QuestionDetailViewController.m

Method - (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex

```
....
345.          if (buttonIndex == 1) {
```

Buffer Size Literal Condition\Path 219:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=219
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 391 of /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m
Line	377	414
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/OnlineTrainViewController.m

Method - (void)examButtonClick:(ExamButton *)sender{

```
....
414.          if (sender.onlineTrainData.left_times.integerValue<1) {
```

Buffer Size Literal Condition\Path 220:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=220
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 62 of

/intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m
Line	377	72
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
72.          }else if (indexPath.row == 1){
```

Buffer Size Literal Condition\Path 221:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=221
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 195 of /intelRetailstore/intelRetailstore/StoreIntegralViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Line	377	210
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Method	- (NSInteger)tableView:(UITableView *)tableView numberOfRowsInSection:(NSInteger)section

```
....
210.          }else if (section ==1) {
```

Buffer Size Literal Condition\Path 222:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=222
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 250 of /intelRetailstore/intelRetailstore/StoreIntegralViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Line	377	272
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Method	- (UIView *)tableView:(UITableView *)tableView viewForHeaderInSection:(NSInteger)section{

```
....
272.          }else if(section == 1){
```

Buffer Size Literal Condition\Path 223:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=223
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 250 of /intelRetailstore/intelRetailstore/StoreIntegralViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Line	377	289
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/StoreIntegralViewController.m

Method - (UIView *)tableView:(UITableView *)tableView viewForHeaderInSection:(NSInteger)section{

```
....
289.          }else if(section == 1){
```

Buffer Size Literal Condition\Path 224:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=224
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 314 of /intelRetailstore/intelRetailstore/StoreIntegralViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Line	377	323
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/StoreIntegralViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
323.          }else if (indexPath.section == 1){
```

Buffer Size Literal Condition\Path 225:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=225
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 314 of /intelRetailstore/intelRetailstore/StoreIntegralViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Line	377	367
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/StoreIntegralViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath

```
....
367.          }else if (indexPath.section == 1){
```

Buffer Size Literal Condition\Path 226:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=226
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 394 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Line	377	417
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m

Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
417.          }else if(type == 1){
```

Buffer Size Literal Condition\Path 227:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=227
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 554 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Line	377	610
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Method	- (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
610.          if (answerIdString.length>1) {
```

Buffer Size Literal Condition\Path 228:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=228
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 565 of /intelRetailstore/GTMBase64/GTMBase64.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/GTMBase64/GTMBase64.m
Line	377	675
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/GTMBase64/GTMBase64.m

Method +(NSUInteger)baseDecode:(const char *)srcBytes

```
....
675.              if (state == 1) {
```

Buffer Size Literal Condition\Path 229:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=229
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 838 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	887
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Method	- (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex{

```
....
887.          }else if (buttonIndex == 1){
```

Buffer Size Literal Condition\Path 230:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=230
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 100 of /intelRetailstore/intelRetailstore/InformationCenter/InformationCenterViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/InformationCenter/InformationCenterViewController.m
Line	377	151
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/InformationCenter/InformationCenterViewController.m
Method	[operationManager GET:informationUrl parameters:nil success:^(AFHTTPRequestOperation *operation, id responseObject) {

```
....
151.                    if (informationData.rec_sts_id.integerValue == 1)
{
```

Buffer Size Literal Condition\Path 231:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=231
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 264 of /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Line	377	303
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
303.          if (onlineTrainData.ifsign.integerValue == 1) {
```

Buffer Size Literal Condition\Path 232:

Severity	Low
Result State	To Verify

Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=232
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 124 of /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Line	377	150
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m

Method - (void)confirmButtonClick:(id)sender {

```
....
150.              if (self.againEnterPassTextField.text.length<1) {
```

Buffer Size Literal Condition\Path 233:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=233
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 83 of /intelRetailstore/intelRetailstore/StoreDetailViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/StoreDetailViewController.m
Line	377	133

Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/StoreDetailViewController.m
Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
133.          if (indexPath.row ==1) {
```

Buffer Size Literal Condition\Path 234:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=234
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 394 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Line	377	469
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
469.              if (optionText.length<1) {
```

Buffer Size Literal Condition\Path 235:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=235
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 680 of /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	377	760
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method	- (BOOL)conditionallyPutRecord:(AWSCognitoRecord *)record datasetName:(NSString*)datasetName withCurrentState:(AWSCognitoRecord *)currentState error:(NSError **)error {

```
....
760.              if(numRows <1){
```

Buffer Size Literal Condition\Path 236:

Severity	Low

Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=236
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 33 of /intelRetailstore/QRcode/QRCodeGenerator.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/QRcode/QRCodeGenerator.m
Line	377	45
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/QRcode/QRCodeGenerator.m

Method + (void)drawQRCode:(QRcode *)code context:(CGContextRef)ctx size:(CGFloat)size {

```
....
45.               if(*data & 1) {
```

Buffer Size Literal Condition\Path 237:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=237
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m

Line	377	282
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m

Method - (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
282.              if (updataSaleData.brand_id.length<1 ) {
```

Buffer Size Literal Condition\Path 238:

Severity Low

Result State To Verify

Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=238

Status New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 264 of /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Line	377	357
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
357.          if (onlineTrainData.ifsign.integerValue == 1) {
```

Buffer Size Literal Condition\Path 239:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=239
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 264 of /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Line	377	434
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
434.          if (onlineTrainData.ifsign.integerValue == 1) {
```

Buffer Size Literal Condition\Path 240:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&pr

	ojectid=10445&pathid=240
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 92 of /intelRetailstore/Pods/Bolts/Bolts/Common/BFTask.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/Bolts/Bolts/Common/BFTask.m
Line	377	109
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/Bolts/Bolts/Common/BFTask.m

Method [task continueWithBlock:^id(BFTask *task) {

```
....
109.                    if (exceptions.count == 1) {
```

Buffer Size Literal Condition\Path 241:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=241
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 264 of /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Line	377	318
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
318.              if (onlineTrainData.iftoday.integerValue == 1) {
```

Buffer Size Literal Condition\Path 242:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=242
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 62 of /intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m
Line	377	87
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/IndividualCenterViewController.m
Method	- (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
87.             if (_locationStr.length<1) {
```

Buffer Size Literal Condition\Path 243:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=243
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 412 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	377	448
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method	- (BFTask *)download:(AWSS3TransferManagerDownloadRequest *)downloadRequest

```
....
448.                 if ([components count] == 1) {
```

Buffer Size Literal Condition\Path 244:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=244

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 92 of /intelRetailstore/Pods/Bolts/Bolts/Common/BFTask.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/Bolts/Bolts/Common/BFTask.m
Line	377	119
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/Bolts/Bolts/Common/BFTask.m

Method [task continueWithBlock:^id(BFTask *task) {

```
....
119.                        if (errors.count == 1) {
```

Buffer Size Literal Condition\Path 245:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=245
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 264 of /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m
Line	377	361
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/IREP/FaceToFaceTrainViewController.m

Method - (UITableViewCell *)tableView:(UITableView *)tableView cellForRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
361.              if (onlineTrainData.ifpass.integerValue == 1) {
```

Buffer Size Literal Condition\Path 246:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=246
Status New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 311 of /intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m
Line	377	342
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m

Method	-(void)collectionView:(UICollectionView *)collectionView didSelectItemAtIndexPath:(NSIndexPath *)indexPath {

```
....
342.          if ([StoreDataArray
sharedInstance].storeDataArray.count>1) {
```

Buffer Size Literal Condition\Path 247:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=247
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 311 of /intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m
Line	377	388
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Menu/MenuCollectionViewController.m
Method	-(void)collectionView:(UICollectionView *)collectionView didSelectItemAtIndexPath:(NSIndexPath *)indexPath {

```
....
388.          if ([StoreDataArray
sharedInstance].storeDataArray.count>1) {
```

Buffer Size Literal Condition\Path 248:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=248

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 154 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	377	155
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method - (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex{

```
....
155.      if (alertView.tag == 200  && buttonIndex == 1) {
```

Buffer Size Literal Condition\Path 249:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=249
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 300 of /intelRetailstore/intelRetailstore/LandinViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/LandinViewController.m

Line	377	308
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method - (IBAction)landInButtonClick:(id)sender {

```
....
308.      if (_userNameTextField.text.length<1 ||
_passwordTextField.text.length<1) {
```

Buffer Size Literal Condition\Path 250:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=250
Status New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 300 of /intelRetailstore/intelRetailstore/LandinViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	377	308
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/LandinViewController.m
Method	- (IBAction)landInButtonClick:(id)sender {

```
....
308.      if (_userNameTextField.text.length<1 ||
_passwordTextField.text.length<1) {
```

Buffer Size Literal Condition\Path 251:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=251
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 372 of /intelRetailstore/intelRetailstore/SurveyDetaiViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Line	377	383
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/SurveyDetaiViewController.m
Method	- (NSInteger)tableView:(UITableView *)tableView numberOfRowsInSection:(NSInteger)section{

```
....
383.      if (type == 0 || type == 1) {
```

Buffer Size Literal Condition\Path 252:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=252

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 471 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m
Line	377	475
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m

Method + (NSString *)getV2StringToSign:(NSMutableURLRequest *)request canonicalizedQueryString:(NSString *)canonicalizedQueryString {

```
....
475.      if (nil == path || [path length] < 1) {
```

Buffer Size Literal Condition\Path 253:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=253
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 613 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m
Line	377	614

Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m
Method - (void)stream:(NSStream *)aStream handleEvent:(NSStreamEvent)eventCode {

```
....
614.      if ((eventCode & (1 << 4))) {
```

Buffer Size Literal Condition\Path 254:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=254
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 59 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/util/AWSMobileAnalyticsStringUtils.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/util/AWSMobileAnalyticsStringUtils.m
Line	377	73
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/util/AWSMobileAnalyticsStringUtils.m
Method	+ (NSString *) trimString: (NSString *) origin_string

```
....
73.      if (str_len > target_length - 1)
```

Buffer Size Literal Condition\Path 255:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=255
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 72 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m
Line	377	139
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m
Method	return [[BFTask taskWithResult:nil] continueWithBlock:^id(BFTask *task) {

```
....
139.          if (!bucketName || [bucketName length] < 1) {
```

Buffer Size Literal Condition\Path 256:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=256

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 72 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m
Line	377	147
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m

Method return [[BFTask taskWithResult:nil] continueWithBlock:^id(BFTask *task) {

```
....
147.          if (!keyName || [keyName length] < 1) {
```

Buffer Size Literal Condition\Path 257:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=257
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 72 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m
Line	377	242
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m
Method	return [[BFTask taskWithResult:nil] continueWithBlock:^id(BFTask *task) {

```
....
242.          if (nil == keyName || [keyName length] < 1) {
```

Buffer Size Literal Condition\Path 258:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=258
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 242 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	377	260
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m

Method	BFTask *uploadTask = [[[initRequest continueWithSuccessBlock:^id(BFTask *task) {

```
....
260.          for (NSInteger i = c; i < partCount + 1; i++) {
```

Buffer Size Literal Condition\Path 259:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=259
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 495 of /intelRetailstore/Pods/XMLDictionary/XMLDictionary/XMLDictionary.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/XMLDictionary/XMLDictionary/XMLDictionary.m
Line	377	497
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/XMLDictionary/XMLDictionary/XMLDictionary.m
Method	- (NSString *)XMLString

```
....
497.      if ([self count] == 1 && ![self nodeName])
```

Buffer Size Literal Condition\Path 260:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=260
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 78 of /intelRetailstore/GData/GDataXMLNode.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/GData/GDataXMLNode.m
Line	377	95
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/GData/GDataXMLNode.m

Method static xmlChar *SplitQNameReverse(const xmlChar *qname, xmlChar **prefix) {

```
....
95.         if (idx < qnameLen - 1) {
```

Buffer Size Literal Condition\Path 261:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=261
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 565 of /intelRetailstore/GTMBase64/GTMBase64.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/GTMBase64/GTMBase64.m
Line	377	639
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/GTMBase64/GTMBase64.m
Method	+(NSUInteger)baseDecode:(const char *)srcBytes

```
....
639.          if ((state == 0) || (state == 1)) {
```

Buffer Size Literal Condition\Path 262:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=262
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 154 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	377	172
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method	- (void)alertView:(UIAlertView *)alertView clickedButtonAtIndex:(NSInteger)buttonIndex{

```
....
172.      }else if(alertView.tag == 1001 && buttonIndex == 1){
```

Buffer Size Literal Condition\Path 263:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=263
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 941 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	377	960
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Method	-(void)removeImageView:(int)indexValue{

```
....
960.          for (int i = indexValue+1; i < self.alreadyPicCount+1;
i++) {
```

Buffer Size Literal Condition\Path 264:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=264

Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 65 of /intelRetailstore/intelRetailstore/EnterViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/EnterViewController.m
Line	377	83
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/EnterViewController.m

Method - (void)setScrollView{

```
....
83.          if (i == _imageArray.count-1) {
```

Buffer Size Literal Condition\Path 265:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=265
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 449 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m
Line	377	462
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m
Method + (NSString *)canonicalizedQueryString:(NSDictionary *)parameters {

```
....
462.          if (index < [sortedKeys count] - 1) {
```

Buffer Size Literal Condition\Path 266:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=266
Status New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 72 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m
Line	377	243
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3PreSignedURL.m
Method return [[BFTask taskWithResult:nil] continueWithBlock:^id(BFTask *task) {

```
....
243.              if (nil == bucketName || [bucketName length] < 1) {
```

Buffer Size Literal Condition\Path 267:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=267
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 564 of /intelRetailstore/GData/GDataXMLNode.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/GData/GDataXMLNode.m
Line	377	571
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/GData/GDataXMLNode.m

Method + (NSString *)localNameForName:(NSString *)name {

```
....
571.        if (range.location + 1 < [name length]) {
```

Buffer Size Literal Condition\Path 268:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=268
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of

/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	276
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m

Method - (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
276.              if (updataSaleData.brand_id.length<1 ||
updataSaleData.mdl_id.length<1 || updataSaleData.cpuModel.length<1){
```

Buffer Size Literal Condition\Path 269:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=269
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 277 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Line	377	445
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Method	- (void)setScrollView{

```
....
445.              }else if(i == (storeDataArray.count+1)){
```

Buffer Size Literal Condition\Path 270:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=270
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 486 of /intelRetailstore/Pods/AWSCognitoSync/Cognito/AWSCognitoDataset.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/AWSCognitoDataset.m
Line	377	524
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/Pods/AWSCognitoSync/Cognito/AWSCognitoDataset.m
Method	return [[self.cognitoService updateRecords:request] continueWithBlock:^id(BFTask *task) {

```
....
524.                            if(record.syncCount.longLongValue >
currentSyncCount.longLongValue + 1){
```

Buffer Size Literal Condition\Path 271:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=271
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 28 of /intelRetailstore/NSData+Base64.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/NSData+Base64.m
Line	377	67
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/NSData+Base64.m

Method - (id) initWithBase64EncodedString:(NSString *) string {

```
....
67.                             if( ( ixinbuf == 1 ) || ( ixinbuf == 2 ) )
ctcharsinbuf = 1;
```

Buffer Size Literal Condition\Path 272:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=272
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 14 of /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Line	377	51
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m

Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
51.      if (typeString[0] == *(@encode(id)) && typeString[1] == '"') {
```

Buffer Size Literal Condition\Path 273:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=273
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	269
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Method	- (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
269.      if (updataSaleData.barcode.length<1 ||
updataSaleData.stor_id.length<1 || updataSaleData.rep_id.length<1 ||
updataSaleData.sessionID.length<1 || ![[NSFileManager
defaultManager]fileExistsAtPath:salesRecord.pic_loc]) {
```

Buffer Size Literal Condition\Path 274:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=274
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 746 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	751
Object	1	1

Code Snippet

File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m

Method	- (void)tableView:(UITableView *)tableView didSelectRowAtIndexPath:(NSIndexPath *)indexPath{

```
....
751.          if ((indexPath.row == _monthArray.count-1)  &&
(self.storeData.role_id.integerValue == STORTYPE_OEM)) {
```

Buffer Size Literal Condition\Path 275:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=275
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	276
Object	1	1

Code Snippet	
File Name	/intelRetailstore/RegexKitLite/RegexKitLite.m
Method	static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Method	- (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
276.              if (updataSaleData.brand_id.length<1 ||
updataSaleData.mdl_id.length<1 || updataSaleData.cpuModel.length<1){
```

Buffer Size Literal Condition\Path 276:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=276
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	276
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m

Method - (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
276.              if (updataSaleData.brand_id.length<1 ||
updataSaleData.mdl_id.length<1 || updataSaleData.cpuModel.length<1){
```

Buffer Size Literal Condition\Path 277:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=277
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 190 of /intelRetailstore/Pods/Bolts/Bolts/iOS/BFWebViewAppLinkResolver.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/Pods/Bolts/Bolts/iOS/BFWebViewAppLinkResolver.m
Line	377	209
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/Pods/Bolts/Bolts/iOS/BFWebViewAppLinkResolver.m
Method - (NSDictionary *)parseALData:(NSArray *)dataArray {

```
....
209.              if (!child || i == nameComponents.count - 1) {
```

Buffer Size Literal Condition\Path 278:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=278
Status New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	269
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m

Method	- (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
269.      if (updataSaleData.barcode.length<1 ||
updataSaleData.stor_id.length<1 || updataSaleData.rep_id.length<1 ||
updataSaleData.sessionID.length<1 || ![[NSFileManager
defaultManager]fileExistsAtPath:salesRecord.pic_loc]) {
```

Buffer Size Literal Condition\Path 279:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=279
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 1400 of /intelRetailstore/GData/GDataXMLNode.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/GData/GDataXMLNode.m
Line	377	1425
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/GData/GDataXMLNode.m

Method + (void)fixQualifiedNamesForNode:(xmlNodePtr)nodeToFix

```
....
1425.              && prefix[prefixLen - 1] == '}') {
```

Buffer Size Literal Condition\Path 280:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=280
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	269
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m

Method - (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
269.      if (updataSaleData.barcode.length<1 ||
updataSaleData.stor_id.length<1 || updataSaleData.rep_id.length<1 ||
updataSaleData.sessionID.length<1 || ![[NSFileManager
defaultManager]fileExistsAtPath:salesRecord.pic_loc]) {
```

Buffer Size Literal Condition\Path 281:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=281
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	377	269

Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Method - (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
269.      if (updataSaleData.barcode.length<1 ||
updataSaleData.stor_id.length<1 || updataSaleData.rep_id.length<1 ||
updataSaleData.sessionID.length<1 || ![[NSFileManager
defaultManager]fileExistsAtPath:salesRecord.pic_loc]) {
```

Buffer Size Literal Condition\Path 282:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=282
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 624 of /intelRetailstore/RegexKitLite/RegexKitLite.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/RegexKitLite/RegexKitLite.m
Line	377	628
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method __attribute__((constructor)) static void rkl_RegisterForLowMemoryNotifications(void) {

```
....
628.    while((rkl_HaveRegisteredForLowMemoryNotifications == 0) &&
((didSwap = OSAtomicCompareAndSwapIntBarrier(0, 1,
&rkl_HaveRegisteredForLowMemoryNotifications)) == false)) { /* Allows
for spurious CAS failures. */ }
```

Buffer Size Literal Condition\Path 283:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=283
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 277 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Line	377	501
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/MainViewController.m

Method - (void)setScrollView{

```
....
501.                    if (((MyStoreData *)[storeDataArray
objectAtIndex:(i-1)]).role_id.integerValue == STORTYPE_DIY) {
```

Buffer Size Literal Condition\Path 284:

Severity	Low

Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=284
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 277 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Line	377	521
Object	1	1

Code Snippet

File Name /intelRetailstore/RegexKitLite/RegexKitLite.m

Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/MainViewController.m

Method - (void)setScrollView{

```
....
521.                    if (((MyStoreData *)[storeDataArray
objectAtIndex:(i-1)]).cat_type_nm.length>0) {
```

Buffer Size Literal Condition\Path 285:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=285
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 277 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m

Line	377	507
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name /intelRetailstore/intelRetailstore/Main/MainViewController.m
Method - (void)setScrollView{

```
....
507.                  }else if (((MyStoreData *)[storeDataArray
objectAtIndex:(i-1)]).role_id.integerValue == STORTYPE_OEM ){
```

Buffer Size Literal Condition\Path 286:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=286
Status	New

The number literal 1 at line 377 of /intelRetailstore/RegexKitLite/RegexKitLite.m specifies the size of a buffer. At line 277 of /intelRetailstore/intelRetailstore/Main/MainViewController.m this number literal is used in conditional statement.

	Source	Destination
File	/intelRetailstore/RegexKitLite/RegexKitLite.m	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Line	377	513
Object	1	1

Code Snippet
File Name /intelRetailstore/RegexKitLite/RegexKitLite.m
Method static const UniChar rkl_emptyUniCharString[1]; // For safety, icu_regexes are 'set' to this when the string they were searched is cleared.

```
....
377.  static const UniChar        rkl_emptyUniCharString[1];
// For safety, icu_regexes are 'set' to this when the string they were
searched is cleared.
```

File Name	/intelRetailstore/intelRetailstore/Main/MainViewController.m
Method	- (void)setScrollView{

```
....
513.                    }else if (((MyStoreData *)[storeDataArray
objectAtIndex:(i-1)]).role_id.integerValue == STORTYPE_MSR){
```

Jailbrake File Referenced By Name

Query Path:
Objc\Cx\Apple Secure Coding Guide\Jailbrake File Referenced By Name Version:0

Description

Jailbrake File Referenced By Name\Path 50:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=50
Status	New

A method writeToFile:atomically: at line 864 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	893	893
Object	writeToFile:atomically:	writeToFile:atomically:

Code Snippet

File Name	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Method	- (void)imagePickerController:(UIImagePickerController *)picker didFinishPickingMediaWithInfo:(NSDictionary *)info

```
....
893.          [imageData writeToFile:filePath atomically:YES];
```

Jailbrake File Referenced By Name\Path 51:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=51
Status	New

A method writeToFile:atomically: at line 150 of /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m
Line	170	170
Object	writeToFile:atomically:	writeToFile:atomically:

Code Snippet
File Name /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m
Method - (IBAction)submitButtonClick:(id)sender {

```
....
170.      [UIImagePNGRepresentation(newImage)writeToFile: filepath
atomically:YES];
```

Jailbrake File Referenced By Name\Path 52:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=52
Status	New

A method writeToURL:atomically: at line 261 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	286	286
Object	writeToURL:atomically:	writeToURL:atomically:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method uploadPartsTask = [uploadPartsTask continueWithSuccessBlock:^id(BFTask *task) {

```
....
286.                  [partData writeToURL:tempURL atomically:YES];
```

Jailbrake File Referenced By Name\Path 53:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=53
Status	New

A method stringWithContentsOfFile:encoding:error: at line 253 of /intelRetailstore/WebViewJavascriptBridge/WebViewJavascriptBridge.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/WebViewJavascriptBridge/WebViewJavascriptBridge.m	/intelRetailstore/WebViewJavascriptBridge/WebViewJavascriptBridge.m
Line	260	260
Object	stringWithContentsOfFile:encoding:error:	stringWithContentsOfFile:encoding:error:

Code Snippet
File Name /intelRetailstore/WebViewJavascriptBridge/WebViewJavascriptBridge.m
Method - (void)webView:(WebView *)webView didFinishLoadForFrame:(WebFrame *)frame

```
....
260.          NSString *js = [NSString stringWithContentsOfFile:filePath
encoding:NSUTF8StringEncoding error:nil];
```

Jailbrake File Referenced By Name\Path 54:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=54
Status	New

A method dataWithContentsOfFile: at line 180 of /intelRetailstore/AFNetworking/AFNetworking/AFSecurityPolicy.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFSecurityPolicy.m	/intelRetailstore/AFNetworking/AFNetworking/AFSecurityPolicy.m
Line	186	186
Object	dataWithContentsOfFile:	dataWithContentsOfFile:

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFSecurityPolicy.m
Method dispatch_once(&onceToken, ^{

```
....
186.              NSData *certificateData = [NSData
dataWithContentsOfFile:path];
```

Jailbrake File Referenced By Name\Path 55:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=55

Status	New

A method dataWithContentsOfFile: at line 45 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m
Line	47	47
Object	dataWithContentsOfFile:	dataWithContentsOfFile:

Code Snippet

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSCredentialsProvider.m

Method + (instancetype)credentialsWithCredentialsFilename:(NSString *)credentialsFilename {

```
....
47.      NSDictionary *credentialsJson = [NSJSONSerialization
JSONObjectWithData:[NSData dataWithContentsOfFile:filePath]
```

Jailbrake File Referenced By Name\Path 56:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=56
Status	New

A method dataWithContentsOfFile: at line 35 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m
Line	43	43
Object	dataWithContentsOfFile:	dataWithContentsOfFile:

Code Snippet

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m

Method + (instancetype)serializerWithResource:(NSString *)resource

```
....
43.          serializer.serviceDefinitionJSON = [NSJSONSerialization
JSONObjectWithData:[NSData dataWithContentsOfFile:filePath]
```

Jailbrake File Referenced By Name\Path 57:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=57
Status	New

A method dataWithContentsOfFile: at line 139 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m
Line	147	147
Object	dataWithContentsOfFile:	dataWithContentsOfFile:

Code Snippet

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m

Method + (instancetype)serializerWithResource:(NSString *)resource actionName:(NSString *)actionName {

```
....
147.          serializer.serviceDefinitionJSON = [NSJSONSerialization
JSONObjectWithData:[NSData dataWithContentsOfFile:filePath]
```

Jailbrake File Referenced By Name\Path 58:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=58
Status	New

A method dataWithContentsOfFile: at line 399 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m

Line	408	408
Object	dataWithContentsOfFile:	dataWithContentsOfFile:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m
Method + (instancetype)serializerWithResource:(NSString *)resource

```
....
408.          serializer.serviceDefinitionJSON = [NSJSONSerialization
JSONObjectWithData:[NSData dataWithContentsOfFile:filePath]
```

Jailbrake File Referenced By Name\Path 59:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=59
Status	New

A method dataWithContentsOfFile: at line 120 of /intelRetailstore/Pods/XMLDictionary/XMLDictionary/XMLDictionary.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/XMLDictionary/XMLDictionary/XMLDictionary.m	/intelRetailstore/Pods/XMLDictionary/XMLDictionary/XMLDictionary.m
Line	122	122
Object	dataWithContentsOfFile:	dataWithContentsOfFile:

Code Snippet
File Name /intelRetailstore/Pods/XMLDictionary/XMLDictionary/XMLDictionary.m
Method - (NSDictionary *)dictionaryWithFile:(NSString *)path

```
....
122.        NSData *data = [NSData dataWithContentsOfFile:path];
```

Jailbrake File Referenced By Name\Path 60:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=60
Status	New

A method createFileAtPath:contents:attributes: at line 112 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m accessing a file by filename.

	Source	Destination

File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Line	130	130
Object	createFileAtPath:contents:attributes:	createFileAtPath:contents:attributes:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Method -(BOOL) createNewFile

```
....
130.      BOOL created = [self.fileManager
createFileAtPath:self.absolutePath
```

Jailbrake File Referenced By Name\Path 61:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=61
Status	New

A method createFileAtPath:contents:attributes: at line 115 of /intelRetailstore/SDWebImage/SDImageCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/SDWebImage/SDImageCache.m	/intelRetailstore/SDWebImage/SDImageCache.m
Line	125	125
Object	createFileAtPath:contents:attributes:	createFileAtPath:contents:attributes:

Code Snippet
File Name /intelRetailstore/SDWebImage/SDImageCache.m
Method - (void)storeKeyWithDataToDisk:(NSArray *)keyAndData

```
....
125.          [fileManager createFileAtPath:[self cachePathForKey:key]
contents:data attributes:nil];
```

Jailbrake File Referenced By Name\Path 62:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=62
Status	New

A method createFileAtPath:contents:attributes: at line 115 of /intelRetailstore/SDWebImage/SDImageCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/SDWebImage/SDImageCache.m	/intelRetailstore/SDWebImage/SDImageCache.m
Line	135	135
Object	createFileAtPath:contents:attributes:	createFileAtPath:contents:attributes:

Code Snippet
File Name /intelRetailstore/SDWebImage/SDImageCache.m
Method - (void)storeKeyWithDataToDisk:(NSArray *)keyAndData

```
....
135.              [fileManager createFileAtPath:[self
cachePathForKey:key] contents:UIImageJPEGRepresentation(image,
(CGFloat)1.0) attributes:nil];
```

Jailbrake File Referenced By Name\Path 63:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=63
Status	New

A method moveItemAtURL:toURL:error: at line 218 of /intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m
Line	228	228
Object	moveItemAtURL:toURL:error:	moveItemAtURL:toURL:error:

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m
Method - (void)URLSession:(NSURLSession *)session

```
....
228.              [[NSFileManager defaultManager] moveItemAtURL:location
toURL:self.downloadFileURL error:&fileManagerError];
```

Jailbrake File Referenced By Name\Path 64:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=64
Status	New

A method moveItemAtURL:toURL:error: at line 999 of /intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m
Line	1009	1009
Object	moveItemAtURL:toURL:error:	moveItemAtURL:toURL:error:

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLSessionManager.m
Method - (void)URLSession:(NSURLSession *)session

```
....
1009.              [[NSFileManager defaultManager]
moveItemAtURL:location toURL:fileURL error:&error];
```

Jailbrake File Referenced By Name\Path 65:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=65
Status	New

A method moveItemAtURL:toURL:error: at line 198 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	206	206
Object	moveItemAtURL:toURL:error:	moveItemAtURL:toURL:error:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method +(BOOL)moveItemAtURLToTrash:(NSURL *)itemURL

```
....
206.      BOOL moved = [[NSFileManager defaultManager]
moveItemAtURL:itemURL toURL:uniqueTrashURL error:&error];
```

Jailbrake File Referenced By Name\Path 66:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=66
Status	New

A method moveItemAtPath:toPath:error: at line 260 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Line	264	264
Object	moveItemAtPath:toPath:error:	moveItemAtPath:toPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Method -(BOOL) renameTo:(NSString *) theNewFilename

```
....
264.      BOOL success = [self.fileManager
moveItemAtPath:self.absolutePath toPath:newAbsolutePath error:&error];
```

Jailbrake File Referenced By Name\Path 67:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=67
Status	New

A method fileExistsAtPath: at line 27 of /intelRetailstore/intelRetailstore/Main/FileSize.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Main/FileSize.m	/intelRetailstore/intelRetailstore/Main/FileSize.m
Line	30	30
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/intelRetailstore/Main/FileSize.m
Method -(long long)fileSize{

```
....
30.      if ([manager fileExistsAtPath:logFilePath]){
```

Jailbrake File Referenced By Name\Path 68:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&pr

	ojectid=10445&pathid=68
Status	New

A method fileExistsAtPath:isDirectory: at line 38 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Line	79	79
Object	fileExistsAtPath:isDirectory:	fileExistsAtPath:isDirectory:

Code Snippet

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m

Method -(id) initWithFileMananager:(NSFileManager*) theFileManager

```
....
79.              BOOL exists = [theFileManager
fileExistsAtPath:self.absolutePath isDirectory:&isDir];
```

Jailbrake File Referenced By Name\Path 69:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=69
Status	New

A method fileExistsAtPath: at line 162 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Line	175	175
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m

Method -(BOOL) exists

```
....
175.      return [self.fileManager fileExistsAtPath:self.absolutePath];
```

Jailbrake File Referenced By Name\Path 70:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=70
Status	New

A method fileExistsAtPath: at line 248 of /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m	/intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Line	269	269
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/intelRetailstore/Declaration/SalesDeclareRecordViewController.m
Method - (void)submitDeclarationWithSalesRecordData:(SalesRecordData *)salesRecord{

```
....
269.      if (updataSaleData.barcode.length<1 ||
updataSaleData.stor_id.length<1 || updataSaleData.rep_id.length<1 ||
updataSaleData.sessionID.length<1 || ![[NSFileManager
defaultManager]fileExistsAtPath:salesRecord.pic_loc]) {
```

Jailbrake File Referenced By Name\Path 71:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=71
Status	New

A method fileExistsAtPath: at line 1691 of /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1692	1692
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet	
File Name	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method	dispatch_sync(self.dispatchQueue, ^{

```
....
1692.          if([[NSFileManager defaultManager] fileExistsAtPath:[self
filePath]])
```

Jailbrake File Referenced By Name\Path 72:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=72
Status	New

A method fileExistsAtPath: at line 76 of /intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m	/intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m
Line	87	87
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet	
File Name	/intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m
Method	- (instancetype)initWithConfiguration:(AWSServiceConfiguration *)configuration

```
....
87.          BOOL fileExistsAtPath = [[NSFileManager defaultManager]
fileExistsAtPath:databaseDirectoryPath];
```

Jailbrake File Referenced By Name\Path 73:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=73
Status	New

A method fileExistsAtPath: at line 412 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m

Line	446	446
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method - (BFTask *)download:(AWSS3TransferManagerDownloadRequest *)downloadRequest

```
....
446.              while ([[NSFileManager defaultManager]
fileExistsAtPath:[NSTemporaryDirectory()
stringByAppendingPathComponent:generatedfileName]]) {
```

Jailbrake File Referenced By Name\Path 74:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=74
Status	New

A method fileExistsAtPath: at line 412 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	474	474
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method - (BFTask *)download:(AWSS3TransferManagerDownloadRequest *)downloadRequest

```
....
474.              if ([[NSFileManager defaultManager]
fileExistsAtPath:tempFileURL.path] == NO) {
```

Jailbrake File Referenced By Name\Path 75:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=75
Status	New

A method fileExistsAtPath: at line 443 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	450	450
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method dispatch_async(_queue, ^{

```
....
450.          if ([[NSFileManager defaultManager]
fileExistsAtPath:[fileURL path]]) {
```

Jailbrake File Referenced By Name\Path 76:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=76
Status New

A method fileExistsAtPath: at line 409 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	417	417
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method dispatch_async(_queue, ^{

```
....
417.          if ([[NSFileManager defaultManager]
fileExistsAtPath:[fileURL path]]) {
```

Jailbrake File Referenced By Name\Path 77:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=77
Status New

A method fileExistsAtPath: at line 182 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	185	185
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method dispatch_once(&predicate, ^{

```
....
185.          if (![[NSFileManager defaultManager]
fileExistsAtPath:[sharedTrashURL path]]) {
```

Jailbrake File Referenced By Name\Path 78:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=78
Status	New

A method fileExistsAtPath: at line 198 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	200	200
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method +(BOOL)moveItemAtURLToTrash:(NSURL *)itemURL

```
....
200.      if (![[NSFileManager defaultManager] fileExistsAtPath:[itemURL
path]])
```

Jailbrake File Referenced By Name\Path 79:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=79
Status	New

A method fileExistsAtPath: at line 235 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	237	237
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method - (BOOL)createCacheDirectory

```
....
237.      if ([[NSFileManager defaultManager]
fileExistsAtPath:[_cacheURL path]])
```

Jailbrake File Referenced By Name\Path 80:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=80
Status	New

A method fileExistsAtPath: at line 306 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	309	309
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Method - (BOOL)removeFileAndExecuteBlocksForKey:(NSString *)key

```
....
309.      if (!fileURL || ![[NSFileManager defaultManager]
fileExistsAtPath:[fileURL path]])
```

Jailbrake File Referenced By Name\Path 81:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=81
Status	New

A method fileExistsAtPath: at line 25 of /intelRetailstore/SDWebImage/SDImageCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/SDWebImage/SDImageCache.m	/intelRetailstore/SDWebImage/SDImageCache.m
Line	36	36
Object	fileExistsAtPath:	fileExistsAtPath:

Code Snippet
File Name /intelRetailstore/SDWebImage/SDImageCache.m
Method - (id)init

```
....
36.          if (![[NSFileManager defaultManager]
fileExistsAtPath:diskCachePath])
```

Jailbrake File Referenced By Name\Path 82:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=82
Status	New

A method attributesOfItemAtPath:error: at line 27 of /intelRetailstore/intelRetailstore/Main/FileSize.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Main/FileSize.m	/intelRetailstore/intelRetailstore/Main/FileSize.m
Line	31	31
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/intelRetailstore/Main/FileSize.m
Method -(long long)fileSize{

```
....
31.          return [[manager attributesOfItemAtPath:logFilePath
error:nil] fileSize];
```

Jailbrake File Referenced By Name\Path 83:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=83
Status	New

A method attributesOfItemAtPath:error: at line 221 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Line	224	224
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsFile.m
Method -(unsigned long long) length

```
....
224.      NSDictionary *attributes = [self.fileManager
attributesOfItemAtPath:self.absolutePath error:&error];
```

Jailbrake File Referenced By Name\Path 84:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=84
Status New

A method attributesOfItemAtPath:error: at line 646 of /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Line	673	673
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Method - (BOOL)appendPartWithFileURL:(NSURL *)fileURL

```
....
673.      NSDictionary *fileAttributes = [[NSFileManager defaultManager]
attributesOfItemAtPath:[fileURL path] error:error];
```

Jailbrake File Referenced By Name\Path 85:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=85
Status New

A method attributesOfItemAtPath:error: at line 170 of /intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m	/intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m
Line	212	212
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m
Method return [[BFTask taskWithResult:nil] continueWithSuccessBlock:^id(BFTask *task) {

```
....
212.          NSDictionary *attributes = [[NSFileManager defaultManager]
attributesOfItemAtPath:databasePath
```

Jailbrake File Referenced By Name\Path 86:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=86
Status	New

A method attributesOfItemAtPath:error: at line 397 of /intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m	/intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m
Line	399	399
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/Kinesis/AWSKinesisRecorder.m
Method - (NSUInteger)diskBytesUsed {

```
....
399.      NSDictionary *attributes = [[NSFileManager defaultManager]
attributesOfItemAtPath:self.databasePath
```

Jailbrake File Referenced By Name\Path 87:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&pr

	ojectid=10445&pathid=87
Status	New

A method attributesOfItemAtPath:error: at line 112 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	145	145
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method - (BFTask *)upload:(AWSS3TransferManagerUploadRequest *)uploadRequest

```
....
145.      NSDictionary *attributes = [[NSFileManager defaultManager]
attributesOfItemAtPath:[[uploadRequest.body path]
stringByResolvingSymlinksInPath]
```

Jailbrake File Referenced By Name\Path 88:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=88
Status	New

A method attributesOfItemAtPath:error: at line 412 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	479	479
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method - (BFTask *)download:(AWSS3TransferManagerDownloadRequest *)downloadRequest

```
....
479.              NSDictionary *attributes = [[NSFileManager
defaultManager] attributesOfItemAtPath:[tempFilePath
stringByResolvingSymlinksInPath]
```

Jailbrake File Referenced By Name\Path 89:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=89
Status	New

A method attributesOfItemAtPath:error: at line 675 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	679	679
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method - (BFTask *)cancel {

```
....
679.          NSDictionary *attributes = [[NSFileManager defaultManager]
attributesOfItemAtPath:[[self.body path]
stringByResolvingSymlinksInPath]
```

Jailbrake File Referenced By Name\Path 90:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=90
Status	New

A method attributesOfItemAtPath:error: at line 694 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	710	710
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method - (BFTask *)pause {

```
....
710.              NSDictionary *attributes = [[NSFileManager
defaultManager] attributesOfItemAtPath:[[self.body path]
stringByResolvingSymlinksInPath]
```

Jailbrake File Referenced By Name\Path 91:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=91
Status	New

A method attributesOfItemAtPath:error: at line 325 of /intelRetailstore/SDWebImage/SDImageCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/SDWebImage/SDImageCache.m	/intelRetailstore/SDWebImage/SDImageCache.m
Line	332	332
Object	attributesOfItemAtPath:error:	attributesOfItemAtPath:error:

Code Snippet
File Name /intelRetailstore/SDWebImage/SDImageCache.m
Method - (void)cleanDisk

```
....
332.          NSDictionary *attrs = [[NSFileManager defaultManager]
attributesOfItemAtPath:filePath error:nil];
```

Jailbrake File Referenced By Name\Path 92:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=92
Status	New

A method setAttributes:ofItemAtPath:error: at line 284 of /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m	/intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m
Line	291	291
Object	setAttributes:ofItemAtPath:error:	setAttributes:ofItemAtPath:error:

Code Snippet
File Name /intelRetailstore/Pods/TMCache/TMCache/TMDiskCache.m

Method	- (BOOL)setFileModificationDate:(NSDate *)date forURL:(NSURL *)fileURL

```
....
291.      BOOL success = [[NSFileManager defaultManager]
setAttributes:@{ NSFileModificationDate: date }
```

Jailbrake File Referenced By Name\Path 93:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=93
Status	New

A method inputStreamWithFileAtPath: at line 315 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m
Line	349	349
Object	inputStreamWithFileAtPath:	inputStreamWithFileAtPath:

Code Snippet	
File Name	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m
Method	-(NSInputStream*) newInputStream:(AWSMobileAnalyticsFile*) theFile

```
....
349.      NSInputStream *inputStream = [NSInputStream
inputStreamWithFileAtPath:file.absolutePath];
```

Jailbrake File Referenced By Name\Path 94:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=94
Status	New

A method inputStreamWithURL: at line 1008 of /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Line	1013	1013

Object	inputStreamWithURL:	inputStreamWithURL:

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Method - (NSInputStream *)inputStream {

```
....
1013.               _inputStream = [NSInputStream
inputStreamWithURL:self.body];
```

Jailbrake File Referenced By Name\Path 95:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=95
Status	New

A method inputStreamWithURL: at line 235 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m
Line	304	304
Object	inputStreamWithURL:	inputStreamWithURL:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Serialization/AWSURLRequestSerialization.m
Method [rules enumerateKeysAndObjectsUsingBlock:^(NSString *memberName, id memberRules, BOOL *stop) {

```
....
304.                            request.HTTPBodyStream = [NSInputStream
inputStreamWithURL:value];
```

Jailbrake File Referenced By Name\Path 96:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=96
Status	New

A method outputStreamToFileAtPath:append: at line 380 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m
Line	411	411
Object	outputStreamToFileAtPath:append:	outputStreamToFileAtPath:append:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m
Method -(NSOutputStream*) newOutputStream:(AWSMobileAnalyticsFile*) theFile

```
....
411.      NSOutputStream *outputStream = [NSOutputStream
outputStreamToFileAtPath: file.absolutePath
```

Jailbrake File Referenced By Name\Path 97:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=97
Status New

A method initWithURL:append: at line 379 of /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m accessing a file by filename.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Line	390	390
Object	initWithURL:append:	initWithURL:append:

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Method - (NSMutableURLRequest *)requestWithMultipartFormRequest:(NSURLRequest *)request

```
....
390.      NSOutputStream *outputStream = [[NSOutputStream alloc]
initWithURL:fileURL append:NO];
```

Unscrubbed Secret

Query Path:
Objc\Cx\Apple Secure Coding Guide\Unscrubbed Secret Version:0
Description

Unscrubbed Secret\Path 118:

Severity Low
Result State To Verify

Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=118
Status	New

	Source	Destination
File	/intelRetailstore/DataMode/RewardData.h	/intelRetailstore/DataMode/RewardData.h
Line	15	15
Object	JingDong_Password	JingDong_Password

Code Snippet
File Name /intelRetailstore/DataMode/RewardData.h
Method @property(nonatomic,copy)NSString *JingDong_Password;

```
....
15.  @property(nonatomic,copy)NSString *JingDong_Password;
```

Unscrubbed Secret\Path 119:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=119
Status	New

	Source	Destination
File	/intelRetailstore/DataMode/RewardData.h	/intelRetailstore/DataMode/RewardData.h
Line	16	16
Object	JingDong_Password_Pay	JingDong_Password_Pay

Code Snippet
File Name /intelRetailstore/DataMode/RewardData.h
Method @property(nonatomic,copy)NSString *JingDong_Password_Pay;

```
....
16.  @property(nonatomic,copy)NSString *JingDong_Password_Pay;
```

Unscrubbed Secret\Path 120:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=120
Status	New

	Source	Destination
File	/intelRetailstore/DataMode/UserData.h	/intelRetailstore/DataMode/UserData.h
Line	35	35

Object	password_force_modify	password_force_modify

Code Snippet
File Name /intelRetailstore/DataMode/UserData.h
Method @property(nonatomic,copy)NSString *password_force_modify;

```
....
35.  @property(nonatomic,copy)NSString *password_force_modify;
```

Unscrubbed Secret\Path 121:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=121
Status New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.h	/intelRetailstore/intelRetailstore/LandinViewController.h
Line	15	15
Object	passwordTextField	passwordTextField

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.h
Method @property (weak, nonatomic) IBOutlet UITextField *passwordTextField;

```
....
15.  @property (weak, nonatomic) IBOutlet UITextField
*passwordTextField;
```

Unscrubbed Secret\Path 122:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=122
Status New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.h	/intelRetailstore/intelRetailstore/LandinViewController.h
Line	17	17
Object	getPasswordButton	getPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.h
Method @property (weak, nonatomic) IBOutlet UIButton *getPasswordButton;

```
....
17.  @property (weak, nonatomic) IBOutlet UIButton *getPasswordButton;
```

Unscrubbed Secret\Path 123:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=123
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.h	/intelRetailstore/intelRetailstore/LandinViewController.h
Line	18	18
Object	rememberPasswordButton	rememberPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.h
Method @property (weak, nonatomic) IBOutlet UIButton *rememberPasswordButton;

```
....
18.  @property (weak, nonatomic) IBOutlet UIButton
*rememberPasswordButton;
```

Unscrubbed Secret\Path 124:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=124
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordViewController.h	/intelRetailstore/intelRetailstore/PasswordViewController.h
Line	15	15
Object	getPasswordButton	getPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/PasswordViewController.h
Method @property (weak, nonatomic) IBOutlet UIButton *getPasswordButton;

```
....
15.  @property (weak, nonatomic) IBOutlet UIButton *getPasswordButton;
```

Unscrubbed Secret\Path 125:

Severity	Low
Result State	To Verify

Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=125
Status	New

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Line	274	274
Object	password	password

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Method - (void)setAuthorizationHeaderFieldWithUsername:(NSString *)username

```
....
274.                                                password:(NSString
*)password
```

Unscrubbed Secret\Path 126:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=126
Status	New

	Source	Destination
File	/intelRetailstore/DataMode/RewardData.m	/intelRetailstore/DataMode/RewardData.m
Line	11	11
Object	_JingDong_Password	_JingDong_Password

Code Snippet
File Name /intelRetailstore/DataMode/RewardData.m
Method @implementation RewardData

```
....
11.  @implementation RewardData
```

Unscrubbed Secret\Path 127:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=127
Status	New

	Source	Destination
File	/intelRetailstore/DataMode/RewardData.m	/intelRetailstore/DataMode/RewardData.m

Line	11	11
Object	_JingDong_Password_Pay	_JingDong_Password_Pay

Code Snippet
File Name /intelRetailstore/DataMode/RewardData.m
Method @implementation RewardData

```
....
11.  @implementation RewardData
```

Unscrubbed Secret\Path 128:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=128
Status New

	Source	Destination
File	/intelRetailstore/DataMode/UserData.m	/intelRetailstore/DataMode/UserData.m
Line	11	11
Object	_password_force_modify	_password_force_modify

Code Snippet
File Name /intelRetailstore/DataMode/UserData.m
Method @implementation UserData

```
....
11.  @implementation UserData
```

Unscrubbed Secret\Path 129:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=129
Status New

	Source	Destination
File	/intelRetailstore/DataMode/UserData.m	/intelRetailstore/DataMode/UserData.m
Line	11	11
Object	setPassword_Force_Modify	setPassword_Force_Modify

Code Snippet
File Name /intelRetailstore/DataMode/UserData.m
Method @implementation UserData

```
....
11.  @implementation UserData
```

Unscrubbed Secret\Path 130:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=130
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Line	18	18
Object	PasswordProtectionViewController	PasswordProtectionViewController

Code Snippet
File Name /intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Method @implementation PasswordProtectionViewController

```
....
18.  @implementation PasswordProtectionViewController
```

Unscrubbed Secret\Path 131:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=131
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/BasicViewController.m	/intelRetailstore/intelRetailstore/BasicViewController.m
Line	50	50
Object	passwordProtectionViewController	passwordProtectionViewController

Code Snippet
File Name /intelRetailstore/intelRetailstore/BasicViewController.m
Method - (void)startPasswordProtectionWithIntervalTime:(NSTimeInterval)timeInterval{

```
....
50.      PasswordProtectionViewController
*passwordProtectionViewController = [storyboard
instantiateViewControllerWithIdentifier:@"PasswordProtectionViewControll
er"];
```

Unscrubbed Secret\Path 132:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=132
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	46
Object	rememberPasswordButton	rememberPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

Unscrubbed Secret\Path 133:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=133
Status New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	46
Object	passwordTextField	passwordTextField

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

Unscrubbed Secret\Path 134:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=134
Status New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	46
Object	_passwordTextField	_passwordTextField

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

Unscrubbed Secret\Path 135:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=135
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	46
Object	_getPasswordButton	_getPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

Unscrubbed Secret\Path 136:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=136
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	46	46
Object	_rememberPasswordButton	_rememberPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method @implementation LandinViewController{

```
....
46.  @implementation LandinViewController{
```

Unscrubbed Secret\Path 137:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=137
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/LandinViewController.m	/intelRetailstore/intelRetailstore/LandinViewController.m
Line	335	335
Object	passwordStr	passwordStr

Code Snippet
File Name /intelRetailstore/intelRetailstore/LandinViewController.m
Method - (IBAction)landInButtonClick:(id)sender {

```
....
335.      NSString *passwordStr = encryptStr;
```

Unscrubbed Secret\Path 138:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=138
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Line	223	223
Object	changePasswordUrl	changePasswordUrl

Code Snippet
File Name /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Method - (void)confirmButtonClick:(id)sender {

```
....
223.      NSString *changePasswordUrl = [NSString
stringWithFormat:URL_CHANGEPASSWORD,[[HostData sharedInstance]
getHost],userName,[UserData sharedInstance].sessionId];
```

Unscrubbed Secret\Path 139:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=139
Status	New

	Source	Destination

File	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Line	12	12
Object	passwordTextFiled	passwordTextFiled

Code Snippet
File Name /intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Method @property (weak, nonatomic) IBOutlet UITextField *passwordTextFiled;

```
....
12.  @property (weak, nonatomic) IBOutlet UITextField
*passwordTextFiled;
```

Unscrubbed Secret\Path 140:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=140
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m	/intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Line	11	11
Object	iPasswordProtectionViewController	iPasswordProtectionViewController

Code Snippet
File Name /intelRetailstore/intelRetailstore/PasswordProtectionViewController.m
Method @interface PasswordProtectionViewController ()<UITextFieldDelegate>

```
....
11.  @interface PasswordProtectionViewController ()<UITextFieldDelegate>
```

Unscrubbed Secret\Path 141:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=141
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordViewController.m	/intelRetailstore/intelRetailstore/PasswordViewController.m
Line	16	16
Object	iPasswordViewController	iPasswordViewController

Code Snippet

File Name	/intelRetailstore/intelRetailstore/PasswordViewController.m
Method	@interface PasswordViewController ()<NetworkRequestDelegate,MBProgressHUDDelegate,UIAlertViewDelegate>

```
....
16.  @interface PasswordViewController
()<NetworkRequestDelegate,MBProgressHUDDelegate,UIAlertViewDelegate>
```

Unscrubbed Secret\Path 142:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=142
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordViewController.m	/intelRetailstore/intelRetailstore/PasswordViewController.m
Line	20	20
Object	PasswordViewController	PasswordViewController

Code Snippet

File Name	/intelRetailstore/intelRetailstore/PasswordViewController.m
Method	@implementation PasswordViewController{

```
....
20.  @implementation PasswordViewController{
```

Unscrubbed Secret\Path 143:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=143
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordViewController.m	/intelRetailstore/intelRetailstore/PasswordViewController.m
Line	20	20
Object	_getPasswordButton	_getPasswordButton

Code Snippet

File Name	/intelRetailstore/intelRetailstore/PasswordViewController.m
Method	@implementation PasswordViewController{

```
....
20.  @implementation PasswordViewController{
```

Unscrubbed Secret\Path 144:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=144
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordViewController.m	/intelRetailstore/intelRetailstore/PasswordViewController.m
Line	34	34
Object	setgetPasswordButton	setgetPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/PasswordViewController.m
Method - (void)setgetPasswordButton{

```
....
34.  - (void)setgetPasswordButton{
```

Unscrubbed Secret\Path 145:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=145
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/PasswordViewController.m	/intelRetailstore/intelRetailstore/PasswordViewController.m
Line	20	20
Object	getPasswordButton	getPasswordButton

Code Snippet
File Name /intelRetailstore/intelRetailstore/PasswordViewController.m
Method @implementation PasswordViewController{

```
....
20.  @implementation PasswordViewController{
```

Unscrubbed Secret\Path 146:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=146
Status	New

	Source	Destination

File	/intelRetailstore/intelRetailstore/PasswordViewController.m	/intelRetailstore/intelRetailstore/PasswordViewController.m
Line	22	22
Object	_isGetPasswordSuccess	_isGetPasswordSuccess

Code Snippet
File Name /intelRetailstore/intelRetailstore/PasswordViewController.m
Method BOOL _isGetPasswordSuccess;

```
....
22.      BOOL _isGetPasswordSuccess;
```

Unscrubbed Secret\Path 147:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=147
Status	New

	Source	Destination
File	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Line	1041	1041
Object	password	password

Code Snippet
File Name /intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Method SecRequestSharedWebCredential((__bridge CFStringRef)domain, (__bridge CFStringRef)account, ^(CFArrayRef credentials, CFErrorRef error) {

```
....
1041.              NSString *password = credential[(__bridge __strong
id)kSecSharedPassword];
```

Unscrubbed Secret\Path 148:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=148
Status	New

	Source	Destination
File	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Line	975	975

Object	password	password

Code Snippet
File Name /intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Method [self.class requestSharedWebCredentialForDomain:domain account:account completion:^(NSArray *credentials, NSError *error) {

```
....
975.                    NSString *password = credential[@"password"];
```

Unscrubbed Secret\Path 149:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=149
Status New

	Source	Destination
File	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Line	950	950
Object	password	password

Code Snippet
File Name /intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Method [self.class requestSharedWebCredentialForDomain:domain account:nil completion:^(NSArray *credentials, NSError *error) {

```
....
950.                    NSString *password = credential[@"password"];
```

Unscrubbed Secret\Path 150:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=150
Status New

	Source	Destination
File	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Line	993	993
Object	password	password

Code Snippet
File Name /intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Method - (void)setSharedPassword:(NSString *)password forAccount:(NSString *)account completion:(void (^)(NSError *error))completion

```
....
993.  - (void)setSharedPassword:(NSString *)password
forAccount:(NSString *)account completion:(void (^)(NSError
*error))completion
```

Unscrubbed Secret\Path 151:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=151
Status	New

	Source	Destination
File	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Line	993	993
Object	setSharedPassword:forAccount:completion:	setSharedPassword:forAccount:completion:

Code Snippet
File Name /intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Method - (void)setSharedPassword:(NSString *)password forAccount:(NSString *)account completion:(void (^)(NSError *error))completion

```
....
993.  - (void)setSharedPassword:(NSString *)password
forAccount:(NSString *)account completion:(void (^)(NSError
*error))completion
```

Unscrubbed Secret\Path 152:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=152
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Line	215	215
Object	oldPwd	oldPwd

Code Snippet
File Name /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Method - (void)confirmButtonClick:(id)sender {

```
....
215.      NSString *oldPwd = oldEncryptStr;
```

Unscrubbed Secret\Path 153:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=153
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m	/intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Line	221	221
Object	newPwd	newPwd

Code Snippet
File Name /intelRetailstore/intelRetailstore/Main/ChangePassViewController.m
Method - (void)confirmButtonClick:(id)sender {

```
....
221.      NSString *newPwd = newEncryptStr;
```

Unscrubbed Secret\Path 154:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=154
Status	New

	Source	Destination
File	/intelRetailstore/DataMode/OnlineTrainData.h	/intelRetailstore/DataMode/OnlineTrainData.h
Line	17	17
Object	pass_rule	pass_rule

Code Snippet
File Name /intelRetailstore/DataMode/OnlineTrainData.h
Method @property(nonatomic,strong)NSNumber *pass_rule;

```
....
17.  @property(nonatomic,strong)NSNumber *pass_rule;
```

Unchecked CString Convertion

Query Path:
Objc\Cx\Apple Secure Coding Guide\Unchecked CString Convertion Version:1

Description

Unchecked CString Convertion\Path 101:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=101
Status	New

The element buffer at line 1113 of /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m contains a C-String that was converted from a CFString object. The length of buffer was not checked after conversion.

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Line	1120	1120
Object	buffer	buffer

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Method - (NSInteger)readData:(NSData *)data

```
....
1120.      [data getBytes:buffer range:range];
```

Unchecked CString Convertion\Path 102:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=102
Status	New

The element expectedDigest at line 150 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m contains a C-String that was converted from a CFString object. The length of expectedDigest was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m
Line	166	166
Object	expectedDigest	expectedDigest

Code Snippet

File Name	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m
Method	-(BOOL)readLine:(NSString**)line withError:(NSError**)readError {

```
....
166.              [decodedData getBytes:expectedDigest
```

Unchecked CString Convertion\Path 103:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=103
Status	New

The element chars at line 38 of /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoUtil.m contains a C-String that was converted from a CFString object. The length of chars was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoUtil.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoUtil.m
Line	43	43
Object	chars	chars

Code Snippet

File Name	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoUtil.m
Method	+ (NSString *)hexEncode:(NSString *)string

```
....
43.      [string getCharacters:chars];
```

Unchecked CString Convertion\Path 104:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=104
Status	New

The element chars at line 65 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m contains a C-String that was converted from a CFString object. The length of chars was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m
Line	69	69

Object	chars	chars

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Authentication/AWSSignature.m
Method + (NSString *)hexEncode:(NSString *)string {

```
....
69.      [string getCharacters:chars];
```

Unchecked CString Convertion\Path 105:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=105
Status	New

The element mutableBytes at line 565 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/XMLWriter/AWSXMLWriter.m contains a C-String that was converted from a CFString object. The length of mutableBytes was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/XMLWriter/AWSXMLWriter.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/XMLWriter/AWSXMLWriter.m
Line	594	594
Object	mutableBytes	mutableBytes

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/XMLWriter/AWSXMLWriter.m
Method - (void) writeEscape:(NSString*)value {

```
....
594.                    [value getCharacters:[data mutableBytes]
range:NSMakeRange(count, length)];
```

Unchecked CString Convertion\Path 106:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=106
Status	New

The element keyPointer at line 50 of /intelRetailstore/CryptLib.m contains a C-String that was converted from a CFString object. The length of keyPointer was not checked after conversion.

	Source	Destination
File	/intelRetailstore/CryptLib.m	/intelRetailstore/CryptLib.m

Line	64	64
Object	keyPointer	keyPointer

Code Snippet
File Name /intelRetailstore/CryptLib.m
Method - (NSData *)encrypt:(NSData *)plainText key:(NSString *)key iv:(NSString *)iv
{

```
....
64.      [key getCString:keyPointer maxLength:sizeof(keyPointer)
encoding:NSUTF8StringEncoding];
```

Unchecked CString Convertion\Path 107:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=107
Status	New

The element ivPointer at line 50 of /intelRetailstore/CryptLib.m contains a C-String that was converted from a CFString object. The length of ivPointer was not checked after conversion.

	Source	Destination
File	/intelRetailstore/CryptLib.m	/intelRetailstore/CryptLib.m
Line	65	65
Object	ivPointer	ivPointer

Code Snippet
File Name /intelRetailstore/CryptLib.m
Method - (NSData *)encrypt:(NSData *)plainText key:(NSString *)key iv:(NSString *)iv
{

```
....
65.      [iv getCString:ivPointer maxLength:sizeof(ivPointer)
encoding:NSUTF8StringEncoding];
```

Unchecked CString Convertion\Path 108:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=108
Status	New

The element keyPointer at line 99 of /intelRetailstore/CryptLib.m contains a C-String that was converted from a CFString object. The length of keyPointer was not checked after conversion.

	Source	Destination
File	/intelRetailstore/CryptLib.m	/intelRetailstore/CryptLib.m
Line	111	111
Object	keyPointer	keyPointer

Code Snippet
File Name /intelRetailstore/CryptLib.m
Method -(NSData *)decrypt:(NSData *)encryptedText key:(NSString *)key iv:(NSString *)iv {

```
....
111.      [key getCString:keyPointer maxLength:sizeof(keyPointer)
encoding:NSUTF8StringEncoding];
```

Unchecked CString Convertion\Path 109:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=109
Status	New

The element ivPointer at line 99 of /intelRetailstore/CryptLib.m contains a C-String that was converted from a CFString object. The length of ivPointer was not checked after conversion.

	Source	Destination
File	/intelRetailstore/CryptLib.m	/intelRetailstore/CryptLib.m
Line	112	112
Object	ivPointer	ivPointer

Code Snippet
File Name /intelRetailstore/CryptLib.m
Method -(NSData *)decrypt:(NSData *)encryptedText key:(NSString *)key iv:(NSString *)iv {

```
....
112.      [iv getCString:ivPointer maxLength:sizeof(ivPointer)
encoding:NSUTF8StringEncoding];
```

Unchecked CString Convertion\Path 110:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=110
Status	New

The element keyPtr at line 85 of /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEnc

ryptedBufferedReader.m contains a C-String that was converted from a CFString object. The length of keyPtr was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m
Line	92	92
Object	keyPtr	keyPtr

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m
Method + (NSData *)AES128EncryptDecrypt:(NSData*)theData

```
....
92.      [key getCString:keyPtr
```

Unchecked CString Convertion\Path 111:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=111
Status New

The element selector at line 12 of /intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m contains a C-String that was converted from a CFString object. The length of selector was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m	/intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m
Line	18	18
Object	selector	selector

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m
Method SEL MTLSelectorWithKeyPattern(NSString *key, const char *suffix) {

```
....
18.   BOOL success = [key getBytes:selector maxLength:keyLength
usedLength:&keyLength encoding:NSUTF8StringEncoding options:0
range:NSMakeRange(0, key.length) remainingRange:NULL];
```

Unchecked CString Convertion\Path 112:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=112

Status	New

The element at line 27 of /intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m contains a C-String that was converted from a CFString object. The length of was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m	/intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m
Line	40	40
Object		

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m
Method SEL MTLSelectorWithCapitalizedKeyPattern(const char *prefix, NSString *key, const char *suffix) {

```
....
40.   BOOL success = [initial getBytes:selector + prefixLength
maxLength:initialLength usedLength:&initialLength
encoding:NSUTF8StringEncoding options:0 range:NSMakeRange(0,
initial.length) remainingRange:NULL];
```

Unchecked CString Convertion\Path 113:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=113
Status	New

The element at line 27 of /intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m contains a C-String that was converted from a CFString object. The length of was not checked after conversion.

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m	/intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m
Line	43	43
Object		

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/MTLReflection.m
Method SEL MTLSelectorWithCapitalizedKeyPattern(const char *prefix, NSString *key, const char *suffix) {

```
....
43.   success = [rest getBytes:selector + prefixLength + initialLength
maxLength:restLength usedLength:&restLength
encoding:NSUTF8StringEncoding options:0 range:NSMakeRange(0,
rest.length) remainingRange:NULL];
```

Unchecked CString Convertion\Path 114:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=114
Status	New

The element cStringUsingEncoding: at line 79 of /intelRetailstore/intelRetailstore/AppDelegate.m contains a C-String that was converted from a CFString object. The length of cStringUsingEncoding: was not checked after conversion.

	Source	Destination
File	/intelRetailstore/intelRetailstore/AppDelegate.m	/intelRetailstore/intelRetailstore/AppDelegate.m
Line	91	91
Object	cStringUsingEncoding:	cStringUsingEncoding:

Code Snippet
File Name /intelRetailstore/intelRetailstore/AppDelegate.m
Method - (void)redirectNSlogToDocumentFolder

```
....
91.      freopen([logFilePath
cStringUsingEncoding:NSASCIIStringEncoding], "a+", stdout);
```

Unchecked CString Convertion\Path 115:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=115
Status	New

The element cStringUsingEncoding: at line 79 of /intelRetailstore/intelRetailstore/AppDelegate.m contains a C-String that was converted from a CFString object. The length of cStringUsingEncoding: was not checked after conversion.

	Source	Destination
File	/intelRetailstore/intelRetailstore/AppDelegate.m	/intelRetailstore/intelRetailstore/AppDelegate.m
Line	93	93
Object	cStringUsingEncoding:	cStringUsingEncoding:

Code Snippet
File Name /intelRetailstore/intelRetailstore/AppDelegate.m
Method - (void)redirectNSlogToDocumentFolder

```
....
93.      freopen([logFilePath
cStringUsingEncoding:NSASCIIStringEncoding], "a+", stderr);
```

Unchecked CString Convertion\Path 116:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=116
Status	New

The element cStringUsingEncoding: at line 42 of /intelRetailstore/intelRetailstore/Main/FileSize.m contains a C-String that was converted from a CFString object. The length of cStringUsingEncoding: was not checked after conversion.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Main/FileSize.m	/intelRetailstore/intelRetailstore/Main/FileSize.m
Line	45	45
Object	cStringUsingEncoding:	cStringUsingEncoding:

Code Snippet
File Name /intelRetailstore/intelRetailstore/Main/FileSize.m
Method - (void)saveLogToDocument{

```
....
45.      freopen([logFilePath
cStringUsingEncoding:NSASCIIStringEncoding], "a+", stdout);
```

Unchecked CString Convertion\Path 117:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=117
Status	New

The element cStringUsingEncoding: at line 42 of /intelRetailstore/intelRetailstore/Main/FileSize.m contains a C-String that was converted from a CFString object. The length of cStringUsingEncoding: was not checked after conversion.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Main/FileSize.m	/intelRetailstore/intelRetailstore/Main/FileSize.m

Line	46	46
Object	cStringUsingEncoding:	cStringUsingEncoding:

Code Snippet
File Name /intelRetailstore/intelRetailstore/Main/FileSize.m
Method - (void)saveLogToDocument{

```
....
46.      freopen([logFilePath
cStringUsingEncoding:NSASCIIStringEncoding], "a+", stderr);
```

Use of Broken or Risky Cryptographic Algorithm

Query Path:
Objc\Cx\ObjectiveC Low Visibility\Use of Broken or Risky Cryptographic Algorithm Version:0

Description

Use of Broken or Risky Cryptographic Algorithm\Path 26:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=26
Status	New

	Source	Destination
File	/intelRetailstore/CryptLib.m	/intelRetailstore/CryptLib.m
Line	151	151
Object	CC_MD5	CC_MD5

Code Snippet
File Name /intelRetailstore/CryptLib.m
Method - (NSString *) md5:(NSString *) input

```
....
151.      CC_MD5( cStr, strlen(cStr), digest ); // This is the md5 call
```

Use of Broken or Risky Cryptographic Algorithm\Path 27:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=27
Status	New

	Source	Destination
File	/intelRetailstore/Hash/NSString+Hashing.m	/intelRetailstore/Hash/NSString+Hashing.m
Line	12	12
Object	CC_MD5	CC_MD5

Code Snippet

File Name /intelRetailstore/Hash/NSString+Hashing.m
Method - (NSString *)MD5Hash

```
....
12.    CC_MD5(cStr, strlen(cStr), result);
```

Use of Broken or Risky Cryptographic Algorithm\Path 28:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=28
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Utility/AWSCategory.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Utility/AWSCategory.m
Line	292	292
Object	CC_MD5	CC_MD5

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/Utility/AWSCategory.m
Method - (NSString *)aws_md5String {

```
....
292.      CC_MD5([dataString bytes], (CC_LONG)[dataString length],
digestArray);
```

Use of Broken or Risky Cryptographic Algorithm\Path 29:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=29
Status New

	Source	Destination
File	/intelRetailstore/SDWebImage/SDImageCache.m	/intelRetailstore/SDWebImage/SDImageCache.m
Line	108	108
Object	CC_MD5	CC_MD5

Code Snippet
File Name /intelRetailstore/SDWebImage/SDImageCache.m
Method - (NSString *)cachePathForKey:(NSString *)key

```
....
108.      CC_MD5(str, (CC_LONG)strlen(str), r);
```

Use of Broken or Risky Cryptographic Algorithm\Path 30:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=30
Status	New

	Source	Destination
File	/intelRetailstore/Hash/NSString+Hashing.m	/intelRetailstore/Hash/NSString+Hashing.m
Line	29	29
Object	CC_MD5_Final	CC_MD5_Final

Code Snippet
File Name /intelRetailstore/Hash/NSString+Hashing.m
Method +(NSString*)dataMD5:(NSData*)data

```
....
29.      CC_MD5_Final(digest, &md5);
```

Use of Broken or Risky Cryptographic Algorithm\Path 31:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=31
Status	New

	Source	Destination
File	/intelRetailstore/Hash/NSString+Hashing.m	/intelRetailstore/Hash/NSString+Hashing.m
Line	58	58
Object	CC_MD5_Final	CC_MD5_Final

Code Snippet
File Name /intelRetailstore/Hash/NSString+Hashing.m
Method +(NSString*)fileMD5:(NSString*)path

```
....
58.      CC_MD5_Final(digest, &md5);
```

Use of Broken or Risky Cryptographic Algorithm\Path 32:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=32
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AW	/intelRetailstore/Pods/AWSiOSSDKv2/AW

	SCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m	SCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m
Line	181	181
Object	CC_SHA1	CC_SHA1

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/io/AWSMobileAnalyticsEncryptedBufferedReader.m
Method -(BOOL)readLine:(NSString**)line withError:(NSError**)readError {

```
....
181.              if(!CC_SHA1([originalData bytes],
(CC_LONG)[originalData length], realDigest) ||
```

Functions Apple Recommends To Avoid

Query Path:
Objc\Cx\ObjectiveC Low Visibility\Functions Apple Recommends To Avoid Version:0

Description

Functions Apple Recommends To Avoid\Path 36:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=36
Status New

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Line	47	47
Object	strncpy	strncpy

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
47.      strncpy(attributes->type, typeString, typeLength);
```

Functions Apple Recommends To Avoid\Path 37:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=37
Status New

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m

Line	65	65
Object	strncpy	strncpy

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
65.             strncpy(trimmedName, className, classNameLength);
```

Functions Apple Recommends To Avoid\Path 38:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=38
Status New

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Line	123	123
Object	strncpy	strncpy

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
123.                    strncpy(selectorString, next, selectorLength);
```

Functions Apple Recommends To Avoid\Path 39:

Severity Low
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=39
Status New

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Line	194	194
Object	strncpy	strncpy

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
194.          strncpy(setterName, "set", 3);
```

Functions Apple Recommends To Avoid\Path 40:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=40
Status	New

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Line	195	195
Object	strncpy	strncpy

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
195.          strncpy(setterName + 3, propertyName, propertyNameLength);
```

Improper Resource Shutdown or Release

Query Path:
Objc\Cx\ObjectiveC Low Visibility\Improper Resource Shutdown or Release Version:0

Description

Improper Resource Shutdown or Release\Path 41:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=41
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m
Line	353	353
Object	inputStream	inputStream

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m
Method -(NSInputStream*) newInputStream:(AWSMobileAnalyticsFile*) theFile

```
....
353.          [inputStream open];
```

Improper Resource Shutdown or Release\Path 42:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=42
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsIOSPreferences.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsIOSPreferences.m
Line	108	108
Object	inputStream	inputStream

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsIOSPreferences.m
Method - (void) loadPreferences {

```
....
108.                  [inputStream open];
```

Improper Resource Shutdown or Release\Path 43:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=43
Status	New

	Source	Destination
File	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m	/intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Line	1148	1148
Object	inputStream	inputStream

Code Snippet
File Name /intelRetailstore/AFNetworking/AFNetworking/AFURLRequestSerialization.m
Method - (BOOL)transitionToNextPhase {

```
....
1148.              [self.inputStream open];
```

Improper Resource Shutdown or Release\Path 44:

Severity	Low

Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=44
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m
Line	416	416
Object	outputStream	outputStream

Code Snippet

File Name /intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/core/system/AWSMobileAnalyticsDefaultFileManager.m

Method -(NSOutputStream*) newOutputStream:(AWSMobileAnalyticsFile*) theFile

```
....
416.          [outputStream open];
```

Use of Hardcoded Password

Query Path:
Objc\Cx\ObjectiveC Low Visibility\Use of Hardcoded Password Version:0

Description

Use of Hardcoded Password\Path 33:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=33
Status	New

	Source	Destination
File	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Line	975	975
Object	password	password

Code Snippet

File Name /intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m

Method [self.class requestSharedWebCredentialForDomain:domain account:account completion:^(NSArray *credentials, NSError *error) {

```
....
975.                  NSString *password = credential[@"password"];
```

Use of Hardcoded Password\Path 34:

Severity	Low

Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=34
Status	New

	Source	Destination
File	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m	/intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Line	950	950
Object	password	password

Code Snippet
File Name /intelRetailstore/Pods/UICKeyChainStore/Lib/UICKeyChainStore/UICKeyChainStore.m
Method [self.class requestSharedWebCredentialForDomain:domain account:nil completion:^(NSArray *credentials, NSError *error) {

```
....
950.                    NSString *password = credential[@"password"];
```

Use of Hardcoded Password\Path 35:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=35
Status	New

	Source	Destination
File	/intelRetailstore/intelRetailstore/BasicViewController.m	/intelRetailstore/intelRetailstore/BasicViewController.m
Line	50	50
Object	passwordProtectionViewController	passwordProtectionViewController

Code Snippet
File Name /intelRetailstore/intelRetailstore/BasicViewController.m
Method - (void)startPasswordProtectionWithIntervalTime:(NSTimeInterval)timeInterval{

```
....
50.      PasswordProtectionViewController
*passwordProtectionViewController = [storyboard
instantiateViewControllerWithIdentifier:@"PasswordProtectionViewControll
er"];
```

Jailbreak Unchecked File Operation Result Code

Query Path:
Objc\Cx\Apple Secure Coding Guide\Jailbreak Unchecked File Operation Result Code Version:0

Description

Jailbreak Unchecked File Operation Result Code\Path 98:

Severity	Low

Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=98
Status	New

The result code of file operation writeToFile:atomically: at line 864 of /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m was ignored.

	Source	Destination
File	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m	/intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m
Line	893	893
Object	writeToFile:atomically:	writeToFile:atomically:

Code Snippet

File Name /intelRetailstore/intelRetailstore/ConsultationWithFeedback/AddQuestionViewController.m

Method - (void)imagePickerController:(UIImagePickerController *)picker didFinishPickingMediaWithInfo:(NSDictionary *)info

```
....
893.          [imageData writeToFile:filePath atomically:YES];
```

Jailbreak Unchecked File Operation Result Code\Path 99:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=99
Status	New

The result code of file operation writeToFile:atomically: at line 150 of /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m was ignored.

	Source	Destination
File	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m	/intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m
Line	170	170
Object	writeToFile:atomically:	writeToFile:atomically:

Code Snippet

File Name /intelRetailstore/intelRetailstore/Declaration/submitModelViewController.m

Method - (IBAction)submitButtonClick:(id)sender {

```
....
170.      [UIImagePNGRepresentation(newImage)writeToFile: filepath
atomically:YES];
```

Jailbreak Unchecked File Operation Result Code\Path 100:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=100
Status	New

The result code of file operation writeToURL:atomically: at line 261 of /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m was ignored.

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m	/intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Line	286	286
Object	writeToURL:atomically:	writeToURL:atomically:

Code Snippet
File Name /intelRetailstore/Pods/AWSiOSSDKv2/S3/AWSS3TransferManager.m
Method uploadPartsTask = [uploadPartsTask continueWithSuccessBlock:^id(BFTask *task) {

```
....
286.                  [partData writeToURL:tempURL atomically:YES];
```

Memory Leak

Query Path:
Objc\Cx\ObjectiveC Low Visibility\Memory Leak Version:0

Description

Memory Leak\Path 46:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=46
Status	New

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Line	40	58
Object	calloc	

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m

Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
40.      mtl_propertyAttributes *attributes = calloc(1,
sizeof(mtl_propertyAttributes) + typeLength + 1);
....
58.              return NULL;
```

Memory Leak\Path 47:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=47
Status	New

	Source	Destination
File	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m	/intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Line	40	210
Object	calloc	

Code Snippet
File Name /intelRetailstore/Pods/Mantle/Mantle/extobjc/EXTRuntimeExtensions.m
Method mtl_propertyAttributes *mtl_copyPropertyAttributes (objc_property_t property) {

```
....
40.      mtl_propertyAttributes *attributes = calloc(1,
sizeof(mtl_propertyAttributes) + typeLength + 1);
....
210.      return NULL;
```

Unchecked Return Value

Query Path:
Objc\Cx\ObjectiveC Low Visibility\Unchecked Return Value Version:0

Description

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=48
Status	New

	Source	Destination
File	/intelRetailstore/GData/GDataXMLNode.m	/intelRetailstore/GData/GDataXMLNode.m
Line	537	537
Object	asprintf	asprintf

Code Snippet
File Name /intelRetailstore/GData/GDataXMLNode.m

Method	- (NSString *)qualifiedName {

```
....
537.        if (asprintf(&qname, "%s:%s", (const char *)xmlNode_->ns->prefix,
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=49
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/AZCommon/ClientContext/AWSMobileAnalyticsIOSClientContext.m	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/AZCommon/ClientContext/AWSMobileAnalyticsIOSClientContext.m
Line	112	112
Object	machine	machine

Code Snippet	
File Name	/intelRetailstore/Pods/AWSiOSSDKv2/AWSCore/MobileAnalytics/AZCommon/ClientContext/AWSMobileAnalyticsIOSClientContext.m
Method	- (NSString *) deviceModelVersionCode

```
....
112.      machine = malloc(len);
```

Dynamic SQL Queries

Query Path:
Objc\Cx\ObjectiveC Best Coding Practice\Dynamic SQL Queries Version:1

Description

Dynamic SQL Queries\Path 288:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=288
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	104	131
Object	stringWithFormat:	UTF8String

Code Snippet

File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
104.          NSString *createString = [NSString stringWithFormat:
....
131.          if(sqlite3_exec(_sqlite, [createString UTF8String], NULL,
NULL, &error) != SQLITE_OK)
```

Dynamic SQL Queries\Path 289:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=289
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	138	160
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
138.          NSString *createString2 = [NSString
stringWithFormat:@"CREATE TABLE IF NOT EXISTS %@ ( \
....
160.          if(sqlite3_exec(_sqlite, [createString2 UTF8String], NULL,
NULL, &error) != SQLITE_OK)
```

Dynamic SQL Queries\Path 290:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=290
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1677	1679
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1677.          NSString *statementString = [NSString
stringWithFormat:@"SELECT %@ FROM %@", columnName, tableName];
....
1679.          if(sqlite3_prepare_v2(self.sqlite, [statementString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 291:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=291
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1606	1612
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1606.          NSString *statementString = [NSString
stringWithFormat:@"DELETE FROM %@ WHERE %@ = ? AND %@ = ?",
AWSCognitoDefaultSqliteDataTableName, AWSCognitoTableIdentityKeyName,
AWSCognitoTableDatasetKeyName];
....
1612.          if(sqlite3_prepare_v2(self.sqlite, [statementString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 292:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=292
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m

Line	1639	1646
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1639.           NSString *sqlString = [NSString stringWithFormat:@"INSERT
OR REPLACE INTO %@(%@,%@,%@,%@) VALUES (?,?,?,?)",
....
1646.           if(sqlite3_prepare_v2(self.sqlite, [sqlString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 293:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=293
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1566	1568
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1566.           NSString *statementString = [NSString
stringWithFormat:@"DELETE FROM %@ WHERE %@=? AND %@=?",
AWSCognitoDefaultSqliteMetadataTableName,
AWSCognitoTableIdentityKeyName, AWSCognitoDatasetFieldName];
....
1568.           if(sqlite3_prepare_v2(self.sqlite, [statementString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 294:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=294
Status New

	Source	Destination

File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1467	1496
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1467.          NSString *updateMetadata = [NSString stringWithFormat:
....
1496.          if((sqlite3_prepare_v2(self.sqlite, [updateMetadata
UTF8String], -1, &updateMetadataStatement, NULL) != SQLITE_OK) ||
```

Dynamic SQL Queries\Path 295:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=295
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1479	1497
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1479.          NSString *updateData = [NSString stringWithFormat:
....
1497.             (sqlite3_prepare_v2(self.sqlite, [updateData
UTF8String], -1, &updateDataStatement, NULL) != SQLITE_OK)) {
```

Dynamic SQL Queries\Path 296:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=296
Status New

	Source	Destination

File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1405	1414
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1405.          NSString *statementString = [NSString
stringWithFormat:@"SELECT %@ FROM %@ WHERE %@ = ? AND %@ LIKE ?",
....
1414.          if(sqlite3_prepare_v2(self.sqlite, [statementString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 297:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=297
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1295	1326
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1295.          NSString *updateMetadata = [NSString stringWithFormat:
....
1326.          if((sqlite3_prepare_v2(self.sqlite, [updateMetadata
UTF8String], -1, &updateMetadataStatement, NULL) != SQLITE_OK) ||
```

Dynamic SQL Queries\Path 298:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=298
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1309	1327
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1309.          NSString *updateData = [NSString stringWithFormat:
....
1327.              (sqlite3_prepare_v2(self.sqlite, [updateData
UTF8String], -1, &updateDataStatement, NULL) != SQLITE_OK)) {
```

Dynamic SQL Queries\Path 299:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=299
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1236	1244
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1236.          NSString *sqlString = [NSString stringWithFormat:@"INSERT
OR REPLACE INTO %@(%@,%@,%@,%@) VALUES (?,?,?,?)",
....
1244.          if(sqlite3_prepare_v2(self.sqlite, [sqlString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 300:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=300
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1199	1207
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1199.           NSString *query = [NSString stringWithFormat:@"SELECT %@
FROM %@ WHERE %@=? AND %@ = ?",
....
1207.           if(sqlite3_prepare_v2(self.sqlite, [query UTF8String], -
1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 301:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=301
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1162	1169
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1162.           NSString *query = [NSString stringWithFormat:@"SELECT
COUNT(*) FROM %@ WHERE %@=? AND %@ = ?",
....
1169.           if(sqlite3_prepare_v2(self.sqlite, [query UTF8String], -
1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 302:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=302

Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	1032	1038
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
1032.           NSString *statementString = [NSString
stringWithFormat:@"DELETE FROM %@ WHERE %@ = ? AND %@ = ? AND %@ = ?",
....
1038.           if(sqlite3_prepare_v2(self.sqlite, [statementString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 303:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=303
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	964	985
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
964.           NSString *sqlString = [NSString stringWithFormat:
....
985.           if(sqlite3_prepare_v2(self.sqlite, [sqlString UTF8String],
-1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 304:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&pr

	ojectid=10445&pathid=304
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	601	641
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
601.          NSString *sqlString = [NSString stringWithFormat:
....
641.          if(sqlite3_prepare_v2(self.sqlite, [sqlString UTF8String],
-1, &statement, NULL) == SQLITE_OK) {
```

Dynamic SQL Queries\Path 305:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=305
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	520	535
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
520.          NSString *query = [NSString stringWithFormat:@"SELECT %@,
%@, %@, %@, %@, %@, %@ FROM %@ WHERE %@ = ? AND %@ = ?",
....
535.          if(sqlite3_prepare_v2(self.sqlite, [query UTF8String], -1,
&statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 306:

Severity	Information
Result State	To Verify

Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=306
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	455	471
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
455.          NSString *query = [NSString stringWithFormat:@"SELECT %@, %@, %@, %@, %@, %@ FROM %@ WHERE %@ != 0 AND %@ = ? AND %@ = ?",
....
471.          if(sqlite3_prepare_v2(self.sqlite, [query UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 307:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=307
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	373	389
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method void (^getRecord)() = ^{

```
....
373.          NSString *query = [NSString stringWithFormat:@"SELECT %@, %@, %@, %@, %@, %@ FROM %@ WHERE %@ = ? AND %@ = ? AND %@ = ?",
....
389.          if(sqlite3_prepare_v2(self.sqlite, [query UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 308:

Severity Information

Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=308
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	326	337
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
326.          NSString *sqlString = [NSString stringWithFormat:@"INSERT
INTO %@(%@,%@,%@,%@,%@,%@,%@) VALUES (?,?,?,?,?,?,?)",
....
337.          if(sqlite3_prepare_v2(self.sqlite, [sqlString UTF8String],
-1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 309:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=309
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	174	182
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
174.          NSString *sqlString = [NSString stringWithFormat:@"INSERT
INTO %@(%@,%@,%@) VALUES (?,?,?)",
....
182.          if(sqlite3_prepare_v2(self.sqlite, [sqlString UTF8String],
-1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 310:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=310
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	67	70
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
67.          NSString *deleteString = [NSString stringWithFormat:
@"DELETE FROM %@ WHERE %@ = ?", AWSCognitoDefaultSqliteDataTableName,
AWSCognitoTableIdentityKeyName];
....
70.          if(sqlite3_prepare_v2(self.sqlite, [deleteString
UTF8String], -1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 311:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=311
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	84	86
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method dispatch_sync(self.dispatchQueue, ^{

```
....
84.          deleteString = [NSString stringWithFormat: @"DELETE FROM %@
WHERE %@ = ?", AWSCognitoDefaultSqliteMetadataTableName,
AWSCognitoTableIdentityKeyName];
....
86.          if(sqlite3_prepare_v2(self.sqlite, [deleteString
UTF8String], -1, &statement, NULL) == SQLITE_OK) {
```

Dynamic SQL Queries\Path 312:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=312
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	696	731
Object	stringWithFormat:	UTF8String

Code Snippet

File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m

Method - (BOOL)conditionallyPutRecord:(AWSCognitoRecord *)record datasetName:(NSString*)datasetName withCurrentState:(AWSCognitoRecord *)currentState error:(NSError **)error {

```
....
696.          NSString *sqlString = [NSString stringWithFormat:
....
731.          if(sqlite3_prepare_v2(self.sqlite, [sqlString UTF8String],
-1, &statement, NULL) == SQLITE_OK) {
```

Dynamic SQL Queries\Path 313:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=313
Status	New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	780	815
Object	stringWithFormat:	UTF8String

Code Snippet

File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method - (BOOL)conditionallyPutRecord:(AWSCognitoRecord *)record datasetName:(NSString*)datasetName withCurrentState:(AWSCognitoRecord *)currentState error:(NSError **)error {

```
....
780.          NSString *sqlString = [NSString stringWithFormat:
....
815.          if(sqlite3_prepare_v2(self.sqlite, [sqlString UTF8String],
-1, &statement, NULL) == SQLITE_OK) {
```

Dynamic SQL Queries\Path 314:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=314
Status New

	Source	Destination
File	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m	/intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Line	860	911
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/AWSCognitoSync/Cognito/Internal/AWSCognitoSQLiteManager.m
Method - (BOOL)conditionallyPutResolvedRecords:(NSArray *) resolvedRecords datasetName:(NSString*)datasetName error:(NSError **)error {

```
....
860.      NSString *sqlString = [NSString stringWithFormat:
....
911.          if(sqlite3_prepare_v2(self.sqlite, [sqlString UTF8String],
-1, &statement, NULL) == SQLITE_OK)
```

Dynamic SQL Queries\Path 315:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=315
Status New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m
Line	140	141
Object	stringWithFormat:	query

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m
Method - (void)setApplicationID:(uint32_t)appID {

```
....
140.      NSString *query = [NSString stringWithFormat:@"pragma
application_id=%d", appID];
141.      FMResultSet *rs = [self executeQuery:query];
```

Dynamic SQL Queries\Path 316:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=316
Status New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m
Line	188	189
Object	stringWithFormat:	query

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m
Method - (void)setUserVersion:(uint32_t)version {

```
....
188.      NSString *query = [NSString stringWithFormat:@"pragma
user_version = %d", version];
189.      FMResultSet *rs = [self executeQuery:query];
```

Dynamic SQL Queries\Path 317:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=317
Status New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	93	876
Object	stringWithFormat:	sql

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabaseAdditions.m
Method - (FMResultSet*)getTableSchema:(NSString*)tableName {

```
....
93.      FMResultSet *rs = [self executeQuery:[NSString
stringWithFormat: @"pragma table_info('%@')", tableName]];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (FMResultSet *)executeQuery:(NSString*)sql, ... {

```
....
876.      id result = [self executeQuery:sql withArgumentsInArray:nil
orDictionary:nil orVAList:args];
```

Dynamic SQL Queries\Path 318:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=318
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	707	933
Object	appendString:	UTF8String

Code Snippet

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (void)extractSQL:(NSString *)sql argumentsList:(va_list)args intoString:(NSMutableString *)cleanedSQL arguments:(NSMutableArray *)arguments {

```
....
707.              [cleanedSQL appendString:@"?"];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (BOOL)executeUpdate:(NSString*)sql error:(NSError**)outErr withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
933.          rc = sqlite3_prepare_v2(_db, [sql UTF8String], -1, &pStmt,
0);
```

Dynamic SQL Queries\Path 319:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=319

Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	707	892
Object	appendString:	sql

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (void)extractSQL:(NSString *)sql argumentsList:(va_list)args intoString:(NSMutableString *)cleanedSQL arguments:(NSMutableArray *)arguments {

```
....
707.                [cleanedSQL appendString:@"?"];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (FMResultSet *)executeQueryWithFormat:(NSString*)format, ... {

```
....
892.      return [self executeQuery:sql withArgumentsInArray:arguments];
```

Dynamic SQL Queries\Path 320:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=320
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	714	933
Object	appendFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (void)extractSQL:(NSString *)sql argumentsList:(va_list)args intoString:(NSMutableString *)cleanedSQL arguments:(NSMutableArray *)arguments {

```
....
714.                [cleanedSQL appendFormat:@"%C", add];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method	- (BOOL)executeUpdate:(NSString*)sql error:(NSError**)outErr withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
933.          rc = sqlite3_prepare_v2(_db, [sql UTF8String], -1, &pStmt,
0);
```

Dynamic SQL Queries\Path 321:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=321
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	714	892
Object	appendFormat:	sql

Code Snippet

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (void)extractSQL:(NSString *)sql argumentsList:(va_list)args intoString:(NSMutableString *)cleanedSQL arguments:(NSMutableArray *)arguments {

```
....
714.              [cleanedSQL appendFormat:@"%C", add];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (FMResultSet *)executeQueryWithFormat:(NSString*)format, ... {

```
....
892.      return [self executeQuery:sql withArgumentsInArray:arguments];
```

Dynamic SQL Queries\Path 322:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=322
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	711	933

Object	appendFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (void)extractSQL:(NSString *)sql argumentsList:(va_list)args intoString:(NSMutableString *)cleanedSQL arguments:(NSMutableArray *)arguments {

```
....
711.                [cleanedSQL appendFormat:@"NULL"];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (BOOL)executeUpdate:(NSString*)sql error:(NSError**)outErr withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
933.          rc = sqlite3_prepare_v2(_db, [sql UTF8String], -1, &pStmt,
0);
```

Dynamic SQL Queries\Path 323:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=323
Status New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	711	892
Object	appendFormat:	sql

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (void)extractSQL:(NSString *)sql argumentsList:(va_list)args intoString:(NSMutableString *)cleanedSQL arguments:(NSMutableArray *)arguments {

```
....
711.                [cleanedSQL appendFormat:@"NULL"];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (FMResultSet *)executeQueryWithFormat:(NSString*)format, ... {

```
....
892.      return [self executeQuery:sql withArgumentsInArray:arguments];
```

Dynamic SQL Queries\Path 324:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=324
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	1273	933
Object	stringWithFormat:	UTF8String

Code Snippet

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (BOOL)releaseSavePointWithName:(NSString*)name error:(NSError**)outErr {

```
....
1273.      NSString *sql = [NSString stringWithFormat:@"release
savepoint '%@';", FMDBEscapeSavePointName(name)];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (BOOL)executeUpdate:(NSString*)sql error:(NSError**)outErr withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
933.          rc = sqlite3_prepare_v2(_db, [sql UTF8String], -1, &pStmt,
0);
```

Dynamic SQL Queries\Path 325:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=325
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	1255	933
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (BOOL)startSavePointWithName:(NSString*)name error:(NSError**)outErr {

```
....
1255.      NSString *sql = [NSString stringWithFormat:@"savepoint
'%@';", FMDBEscapeSavePointName(name)];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (BOOL)executeUpdate:(NSString*)sql error:(NSError**)outErr withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
933.          rc = sqlite3_prepare_v2(_db, [sql UTF8String], -1, &pStmt,
0);
```

Dynamic SQL Queries\Path 326:

Severity Information
Result State To Verify
Online Results https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=326
Status New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	1287	933
Object	stringWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (BOOL)rollbackToSavePointWithName:(NSString*)name error:(NSError**)outErr {

```
....
1287.      NSString *sql = [NSString stringWithFormat:@"rollback
transaction to savepoint '%@';", FMDBEscapeSavePointName(name)];
```

File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m

Method - (BOOL)executeUpdate:(NSString*)sql error:(NSError**)outErr withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
933.          rc = sqlite3_prepare_v2(_db, [sql UTF8String], -1, &pStmt,
0);
```

Dynamic SQL Queries\Path 327:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=327
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	786	793
Object	initWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (FMResultSet *)executeQuery:(NSString *)sql withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
786.                NSString *parameterName = [[NSString alloc] initWithFormat:@":%@", dictionaryKey];
....
793.                int namedIdx = sqlite3_bind_parameter_index(pStmt, [parameterName UTF8String]);
```

Dynamic SQL Queries\Path 328:

Severity	Information
Result State	To Verify
Online Results	https://checkmarx.intel.com/CxWebClient/ViewerMain.aspx?scanid=47704&projectid=10445&pathid=328
Status	New

	Source	Destination
File	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m	/intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Line	968	974
Object	initWithFormat:	UTF8String

Code Snippet
File Name /intelRetailstore/Pods/FMDB/src/fmdb/FMDatabase.m
Method - (BOOL)executeUpdate:(NSString*)sql error:(NSError**)outErr withArgumentsInArray:(NSArray*)arrayArgs orDictionary:(NSDictionary *)dictionaryArgs orVAList:(va_list)args {

```
....
968.                NSString *parameterName = [[NSString alloc] initWithFormat:@":%@", dictionaryKey];
....
974.                int namedIdx = sqlite3_bind_parameter_index(pStmt, [parameterName UTF8String]);
```

Reflected XSS All Clients

Risk

What might happen

An attacker could use social engineering to cause a user to send the website engineered input, rewriting web pages and inserting malicious scripts. The attacker can then pretend to be the original website, which would enable the attacker to steal the user's password, request the user’s credit card information, provide false information, or run malware. From the victim’s point of view, this is the original website, and the victim would blame the site for incurred damage.

Cause

How does it happen

The application creates web pages that include data from previous user input. The user input is embedded directly in the page's HTML, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of embedding arbitrary user input without first encoding it in a format that would prevent the browser from treating it like HTML instead of plain text.

General Recommendations

How to avoid it

1. 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 2. Fully encode all dynamic data before embedding it in output. 3. Encoding should be context-sensitive. For example: ● HTML encoding for HTML content ● HTML Attribute encoding for data output to attribute values ● JavaScript encoding for server-generated JavaScript 4. Consider using either the ESAPI encoding library, or the built-in platform functions. For earlier versions of ASP.NET, consider using the AntiXSS library. 5. In the Content-Type HTTP response header, explicitly define character encoding (charset) for the entire page. 6. Set the httpOnly flag on the session cookie, to prevent XSS exploits from stealing the cookie.

Source Code Examples

CSharp

The application uses the "Referer" field string to construct the HttpResponse

```
public class ReflectedXssAllClients
{
        public static void foo(HttpRequest Request, HttpResponse Response)
        {
                string Referer = Request.QueryString["Referer"];
                Response.BinaryWrite(Referer);
        }
}
```

The "Referer" field string is HTML encoded before use

```
public class ReflectedXssAllClientsFixed
{
        public static void foo(HttpRequest Request, HttpResponse Response,
AntiXss.AntiXssEncoder encoder)
        {
                string Referer = Request.QueryString["Referer"];
                Response.BinaryWrite(encoder.HtmlEncode(Referer, true));
        }
}
```

User input is written to a TextBox displayed on the screen enabling a user to inject a script

```
public class ReflectedXSSSpecificClients
{
        public void foo(TextBox tb)
        {
                string input = Console.ReadLine();
                tb.Text = input;
        }
}
```

The user input is Html encoded before being displayed on the screen

```
public class ReflectedXSSSpecificClientsFixed
{
        public void foo(TextBox tb, AntiXssEncoder encode)
        {
                string input = Console.ReadLine();
                tb.Text = encode.HtmlEncode(input);
        }
```

```
}
```

The application uses the "filename" field string from an HttpRequest construct an HttpResponse

```
public class UTF7XSS
{
        public void foo(HttpRequest Request, HttpResponse Response
        {
                Response.Charset("UTF-7");
                string filename = Request.QueryString["filename"];
                Response.BinaryWrite(AntiXss.HtmlEncode(filename));
        }
}
```

The "filename" string is converted to an int and using a switch case the new "filename" string is constructed

```
public class UTF7XSSFixed
{
        public static void foo(HttpRequest Request, HttpResponse Response)
        {
                Response.Charset("UTF-7");
                string filename = Request.QueryString["fileNum"];
                int fileNum = Convert.ToInt32(filename);

                switch(fileNum)
                {
                        case 1:
                                filename = "File1.txt";
                                break;
                        default:
                                filename = "File2.txt";
                                break;
                }

                Response.BinaryWrite(AntiXss.HtmlEncode(filename));
        }
}
```

Java

User input is written to a label displayed on the screen enabling a user to inject a script

```
public class ReflectedXSSAllClients {
	public static void XSSExample(TextArea name) {
		Label label = new Label();
		label.setText("Hello " + name.getText());
	}
}
```

Switch case is used in order to assemble the label's text value and manage wrong user input

```
public class ReflectedXSSAllClientsFixed {
	public static void XSSExample(TextArea name) {
		Label label = new Label();
		switch (name) {
		case "Joan":
			label.setText("Hello Joan");
			break;
		case "Jim":
			label.setText("Hello Jim");
			break;
		case "James":
			label.setText("Hello James");
			break;
		default:
			System.out.println("Wrong Input");
		}
	}
}
```

Stored XSS

Risk

What might happen

An attacker could use legitimate access to the application to submit engineered data to the application's database. When another user subsequently accesses this data, web pages may be rewritten and malicious scripts may be activated.

Cause

How does it happen

The application creates web pages that include data from the application's database. The data is embedded directly in the page's HTML, causing the browser to display it as part of the web page. This data may have originated in input from another user. If the data includes HTML fragments or Javascript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of embedding arbitrary database data without first encoding it in a format that would prevent the browser from treating it like HTML instead of plain text.

General Recommendations

How to avoid it

1. Validate all dynamic data, 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 2. Validation is not a replacement for encoding. Fully encode all dynamic data, regardless of source, before embedding it in output. Encoding should be context-sensitive. For example: ● HTML encoding for HTML content ● HTML attribute encoding for data output to attribute values ● Javascript encoding for server-generated Javascript 3. Consider using either the ESAPI encoding library, or its built-in functions. For earlier versions of ASP.NET, consider using the AntiXSS library. 4. In the Content-Type HTTP response header, explicitly define character encoding (charset) for the entire page. 5. Set the httpOnly flag on the session cookie, to prevent XSS exploits from stealing the cookie.

Source Code Examples

CSharp

Data obtained from the excecution of an SQL command is outputed to a label

```
public class StoredXss
{
        public string foo(Label lblOutput, SqliteConnection connection, string id)
        {
                string sql = "select email from CustomerLogin where customerNumber = " + id;
                SqliteCommand cmd = new SqliteCommand(sql, connection);
                string output = (string)cmd.ExecuteScalar();
                lblOutput.Text = String.IsNullOrEmpty(output) ? "Customer Number does not
exist" : output;
        }
}
```

The outputed string is Html encoded before it is displayed in the label

```
public class StoredXssFixed
{
        public string foo(Label lblOutput, SqliteConnection connection, HttpServerUtility
Server, string id)
        {
                SqliteConnection connection = new SqliteConnection(connectionString)
                string sql = "select email from CustomerLogin where customerNumber = " + id;
                SqliteCommand cmd = new SqliteCommand(sql, connection);
                string output = (string)cmd.ExecuteScalar();
                lblOutput.Text = String.IsNullOrEmpty(output) ? "Customer Number does not
exist" : Server.HtmlEncode(output);
        }
}
```

Java

Data obtained from the excecution of an SQL command is outputed to a label

```
public class Stored_XSS {
      public static void XSSExample(Statement stmt) throws SQLException {
            Label label = new Label();
            ResultSet rs;
            rs = stmt.executeQuery("SELECT * FROM Customers WHERE UserName = Mickey");
            String lastNames = "";
            while (rs.next()) {
                  lastNames += rs.getString("Lname") + ", ";
            }
            label.setText("Mickey last names are: " + lastNames + " ");
      }
}
```

The outputed string is encoded to hard-coded string before it is displayed in the label

```
public class Stored_XSS_Fix {
      public static void XSSExample(Statement stmt) throws SQLException {
            Label label = new Label();
            ResultSet rs;
            HashMap<String, String> sanitize = new HashMap<String, String>();
            sanitize.put("A", "Cohen");
            sanitize.put("B", "Smith");
            sanitize.put("C", "Bond");
            rs = stmt.executeQuery("SELECT * FROM Customers WHERE UserName = Mickey");
            String lastNames = "";
            while (rs.next()) {
                  lastNames += sanitize.get(rs.getString("Lname")) + ", ";
            }
            label.setText("Mickey last names are: " + lastNames + " ");
      }
}
```

Buffer Size Literal Overflow

Risk

What might happen

An attacker can exploit the buffer overflow to execute an arbitrary code with the privileges of the vulnerable application.

Cause

How does it happen

The overflown buffer is allocated in the stack. Right after the end of the buffer, the function 'return address' is located. An attacker manipulates the input in such a way that when data is written into the buffer the return address is overwritten. The new return address points to a memory segment under the attackers control. When the function returns, the attackers code is executed with the application privileges.

General Recommendations

How to avoid it

1. Define a constant that holds the buffer size, then use this constant throughout the code. Carefully check if the <= comparison operator is suitable.

Source Code Examples

Objc

Code example that is vulnerable to buffer overflow

```
void f(){
    char buf[10];
    char* sourceString = istream.read("input");
    if (strlen(sourceString) <= 10)
    {
        strcpy(buf,sourceString);
    }
}
```

Code that is resilient to buffer overflow

```
void f()
{
    const int MAX_INPUT_SIZE = 256;
    const int BUFFER_SIZE = 10;
    char buf[BUFFER_SIZE];
    char* sourceString = istream.read("input");
    if (strnlen(sourceString,MAX_INPUT_SIZE) < BUFFER_SIZE)
```

```
    {
        strcpy(buf,sourceString);
    }
}
```

Third Party Keyboards On Sensitive Field

Risk

What might happen

A malicious third party keyboard may perform key-logging and transmit the logged information to an attacker’s server. By default, all UITextField and UITextView objects with the secureTextEntry property set to YES disallow the usage of third party keyboards. However, if secureTextEntry is set to NO, to make the characters visible for example, a third party keyboard may steal sensitive data.

Cause

How does it happen

The user installs a malicious third party keyboard that presents itself as legitimate. The user taps a UITextField in the application UI to enter his social security number. The UITextField has its secureTextEntry property set to NO, so that typed-in characters are visible. In this case, third party keyboards are available for use. The user chooses to use the malicious keyboard. The keyboard logs the entered social security number and sends it to an attacker's server.
NOTE: The secureTextEntry property can also be set from XIB file, in this case the a false positive result may be reported.

General Recommendations

How to avoid it

1. Mark the UITextView and UITextField objects that contain sensitive data as secure by setting the secureTextEntry property to YES. See example “Marking a UITextField as secure”. -Or-
2. Disable the usage of third party keyboards entirely in your application. Note that this may degrade the user experience of your application. See example “To disabling third party keyboards, add the following code to your UIApplicationDelegate”.

Source Code Examples

Objc

Marking a UITextField as secure

```
UITextField* textField = [[UITextFieldalloc] init];
textField.secureTextEntry = YES;
```

To disabling third party keyboards, add the following code to your UIApplicationDelegate

```
-(BOOL)application:(UIApplication *)application shouldAllowExtensionPointIdentifier:(NSString
*)extensionPointIdentifier
{

    if (extensionPointIdentifier == UIApplicationKeyboardExtensionPointIdentifier)
    {
        return NO;
    }

    return YES;
}
```

Cut And Paste Leakage

Risk

What might happen

An attacker could get access to the data stored in the cut and paste buffer. If sensitive data was stored in the buffer, it could be leaked.

Cause

How does it happen

The application shows some sensitive data on a screen, such as a credit card number, using a UI element that allows copying its contents to the paste buffer. The user finishes using the application, and closes it. The sensitive data remains in the paste buffer. An attacker steals the mobile device, and pastes this data into some other application, such as email.
NOTE: The secureTextEntry property can also be set from XIB file, in this case the a false positive result may be reported.

General Recommendations

How to avoid it

1. Mark UITextView and UITextField that contain sensitive data as secure by setting the secureTextEntry property to YES. -Or-
2. Disable the “copy” action on UITextView and UITextField instances that contain sensitive data. -Or-
3. Clear the paste board buffer just before the application moves to the background. Listen to UIApplicationDidEnterBackgroundNotification or implement an applicationDidEnterBackground: method in UIApplicationDelegate, and clear the paste board using this method.

Source Code Examples

Objc

To disable the copy action on UITextField, implement a new class inheriting from UITextFiled, and implement canPerformAction:withSender:

```
/* CXTextField.h file */

#import <Foundation/Foundation.h>

#import <UIKit/UIKit.h>

@interface CXTextField : UITextField

@end

/* CXTextField.m file */

#import "CXTextField.h"
```

```
@implementation CXTextField

- (BOOL)canPerformAction:(SEL)action withSender:(id)sender
{

if (sender == [UIApplicationsharedApplication] &&
    (action == @selector(copy:) || action == @selector(cut:))) {
        return NO;
    } else {
        return [super canPerformAction:actionwithSender:sender];
    }
}


@end
```

The example below shows how to clear the paste buffer just before the application goes to background:

```
- (void)viewDidLoad
{

    [[NSNotificationCenterdefaultCenter] addObserver:self
                                selector:@selector(didEnterBackground:)
                                name:UIApplicationDidEnterBackgroundNotification
                          object:nil];
}

-(void)didEnterBackground:(NSNotification *)notification
{

UIPasteboard *pasteboard = [UIPasteboardgeneralPasteboard];
pasteboard.string = @"";
}
```

Marking a UITextField as secure:

```
UITextField* textField = [[UITextFieldalloc] init];
textField.secureTextEntry = YES;
```

Insecure Storage of Sensitive Information

Weakness ID: 922 *(Weakness Class)* **Status:** Incomplete

Description

Description Summary

The software stores sensitive information without properly limiting read or write access by unauthorized actors.

Extended Description

If read access is not properly restricted, then attackers can steal the sensitive information. If write access is not properly restricted, then attackers can modify and possibly delete the data, causing incorrect results and possibly a denial of service.

Time of Introduction

- Architecture and Design
- Implementation
- System Configuration

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Confidentiality	Technical Impact: *Read application data; Read files or directories* Attackers can read sensitive information by accessing the unrestricted storage mechanism.
Integrity	Technical Impact: *Modify application data; Modify files or directories* Attackers can read sensitive information by accessing the unrestricted storage mechanism.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	664		**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	312		Development Concepts699 Research Concepts1000
ParentOf	Weakness Base	921		**Development Concepts (primary)699** **Research Concepts (primary)1000**

Relationship Notes

There is an overlapping relationship between insecure storage of sensitive information () and missing encryption of sensitive information (). Encryption is often used to prevent an attacker from reading the sensitive data. However, encryption does not prevent the attacker from erasing or overwriting the data.

Maintenance Notes

This is a high-level node that includes children from various parts of the CWE research view (). Currently, most of the information is in these child entries. This entry will be made more comprehensive in later CWE versions.

Content History

Submissions

Submission Date	Submitter	Organization	Source
2013-06-23	MITRE		Internal CWE Team

ReDoS

Risk

What might happen

The regular expression Denial of Service (ReDoS) is a Denial of Service attack, that exploits the fact that most regular expression implementations may reach a critical mass that cause them to work very slowly (exponentially related to input size). An attacker can then cause a program using a regular expressions to access at these critical mass periods and then hang for a very long time.

Cause

How does it happen

The Problematic Regex Naive Algorithm The regular expression naive algorithm builds a Nondeterministic Finite Automaton (NFA), which is a finite state machine for which each pair of state and input symbols there may be several possible outcomes. When the engine starts to make transitions towards the end of the input, several possible next states according to a deterministic algorithm can be used. This algorithm tries one-by-one using all the possible paths (if needed) until a match is found (or all the paths have been tried and have failed). Note: Not all algorithms are naive, and usually regex algorithms can be written in an efficient way. Unfortunately, most regex engines today try to solve not only pure regexes, but also expanded regexes with "special additions", such as back-references that cannot always be solved efficiently. So even if the regex is not expanded, a naive algorithm is used. See more information at: https://www.owasp.org/index.php/Regular_expression_Denial_of_Service_-_ReDoS Evil Regexes A regex is called "evil" if it gets stuck on crafted input. Evil regex patterns contain: • Grouping with repetition • Inside the repeated group: • Repetition • Alternation with overlapping Examples of Evil Patterns: • (a+)+ • ([a-zA-Z]+)* • (a

General Recommendations

How to avoid it

aa)+ • (a

Source Code Examples

Missing Encryption of Sensitive Data

Weakness ID: 311 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not encrypt sensitive or critical information before storage or transmission.

Extended Description

The lack of proper data encryption passes up the guarantees of confidentiality, integrity, and accountability that properly implemented encryption conveys.

Time of Introduction

- Architecture and Design
- Operation

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Confidentiality	If the application does not use a secure channel, such as SSL, to exchange sensitive information, it is possible for an attacker with access to the network traffic to sniff packets from the connection and uncover the data. This attack is not technically difficult, but does require physical access to some portion of the network over which the sensitive data travels. This access is usually somewhere near where the user is connected to the network (such as a colleague on the company network) but can be anywhere along the path from the user to the end server.
Confidentiality Integrity	Omitting the use of encryption in any program which transfers data over a network of any kind should be considered on par with delivering the data sent to each user on the local networks of both the sender and receiver. Worse, this omission allows for the injection of data into a stream of communication between two parties -- with no means for the victims to separate valid data from invalid. In this day of widespread network attacks and password collection sniffers, it is an unnecessary risk to omit encryption from the design of any system which might benefit from it.

Likelihood of Exploit

High to Very High

Detection Methods

Manual Analysis

The characterizaton of sensitive data often requires domain-specific understanding, so manual methods are useful. However, manual efforts might not achieve desired code coverage within limited time constraints. Black box methods may produce artifacts (e.g. stored data or unencrypted network transfer) that require manual evaluation.

Effectiveness: High

Automated Analysis

Automated measurement of the entropy of an input/output source may indicate the use or lack of encryption, but human analysis is still required to distinguish intentionally-unencrypted data (e.g. metadata) from sensitive data.

Demonstrative Examples

Example 1

The following code attempts to establish a connection, read in a password, then store it to a buffer.

(Bad Code)

Example Language: **C**

```
server.sin_family = AF_INET; hp = gethostbyname(argv[1]);
if (hp==NULL) error("Unknown host");
memcpy( (char *)&server.sin_addr,(char *)hp->h_addr,hp->h_length);
if (argc < 3) port = 80;
else port = (unsigned short)atoi(argv[3]);
```

```
server.sin_port = htons(port);
if (connect(sock, (struct sockaddr *)&server, sizeof server) < 0) error("Connecting");
...
while ((n=read(sock,buffer,BUFSIZE-1))!=-1) {

write(dfd,password_buffer,n);
...
```

While successful, the program fails to encrypt the data before writing it to a buffer, possibly exposing it to unauthorized actors.

Example 2

The following code attempts to establish a connection to a site to communicate sensitive information.

(Bad Code)

Example Language: **Java**

```
try {
URL u = new URL("http://www.secret.example.org/");
HttpURLConnection hu = (HttpURLConnection) u.openConnection();
hu.setRequestMethod("PUT");
hu.connect();
OutputStream os = hu.getOutputStream();
hu.disconnect();
}
catch (IOException e) {
//...
}
```

Though a connection is successfully made, the connection is unencrypted and it is possible that all sensitive data sent to or received from the server will be read by unintended actors.

Observed Examples

Reference	Description
CVE-2009-2272	password and username stored in cleartext in a cookie
CVE-2009-1466	password stored in cleartext in a file with insecure permissions
CVE-2009-0152	chat program disables SSL in some circumstances even when the user says to use SSL.
CVE-2009-1603	Chain: product uses an incorrect public exponent when generating an RSA key, which effectively disables the encryption
CVE-2009-0964	storage of unencrypted passwords in a database
CVE-2008-6157	storage of unencrypted passwords in a database
CVE-2008-6828	product stores a password in cleartext in memory
CVE-2008-1567	storage of a secret key in cleartext in a temporary file
CVE-2008-0174	SCADA product uses HTTP Basic Authentication, which is not encrypted
CVE-2007-5778	login credentials stored unencrypted in a registry key
CVE-2002-1949	Passwords transmitted in cleartext.
CVE-2008-4122	Chain: failure to set "secure" flag in HTTPS cookie causes it to be transmitted across unencrypted HTTP.
CVE-2008-3289	Product sends password hash in cleartext in violation of intended policy.

CVE-2008-4390	Remote management feature sends sensitive information including passwords in cleartext.
CVE-2007-5626	Backup routine sends password in cleartext in email.
CVE-2004-1852	Product transmits Blowfish encryption key in cleartext.
CVE-2008-0374	Printer sends configuration information, including administrative password, in cleartext.
CVE-2007-4961	Chain: cleartext transmission of the MD5 hash of password enables attacks against a server that is susceptible to replay (CWE-294).
CVE-2007-4786	Product sends passwords in cleartext to a log server.
CVE-2005-3140	Product sends file with cleartext passwords in e-mail message intended for diagnostic purposes.

Potential Mitigations

Phase: Requirements

Clearly specify which data or resources are valuable enough that they should be protected by encryption. Require that any transmission or storage of this data/resource should use well-vetted encryption algorithms.

Phase: Architecture and Design

Using threat modeling or other techniques, assume that your data can be compromised through a separate vulnerability or weakness, and determine where encryption will be most effective. Ensure that data you believe should be private is not being inadvertently exposed using weaknesses such as insecure permissions (CWE-732).

Phase: Architecture and Design

Ensure that encryption is properly integrated into the system design, including but not necessarily limited to:

- Encryption that is needed to store or transmit private data of the users of the system
- Encryption that is needed to protect the system itself from unauthorized disclosure or tampering

Identify the separate needs and contexts for encryption:

- One-way (i.e., only the user or recipient needs to have the key). This can be achieved using public key cryptography, or other techniques in which the encrypting party (i.e., the software) does not need to have access to a private key.
- Two-way (i.e., the encryption can be automatically performed on behalf of a user, but the key must be available so that the plaintext can be automatically recoverable by that user). This requires storage of the private key in a format that is recoverable only by the user (or perhaps by the operating system) in a way that cannot be recovered by others.

Phase: Architecture and Design

Do not develop your own cryptographic algorithms. They will likely be exposed to attacks that are well-understood by cryptographers. Reverse engineering techniques are mature. If your algorithm can be compromised if attackers find out how it works, then it is especially weak.

Phase: Architecture and Design

Select a well-vetted algorithm that is currently considered to be strong by experts in the field, and select well-tested implementations.

For example, US government systems require FIPS 140-2 certification.

As with all cryptographic mechanisms, the source code should be available for analysis.

Periodically ensure that you aren't using obsolete cryptography. Some older algorithms, once thought to require a billion years of computing time, can now be broken in days or hours. This includes MD4, MD5, SHA1, DES, and other algorithms which were once regarded as strong.

Phase: Architecture and Design

Compartmentalize your system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area.

Phases: Implementation; Architecture and Design

When you use industry-approved techniques, you need to use them correctly. Don't cut corners by skipping resource-intensive steps (CWE-325). These steps are often essential for preventing common attacks.

Phase: Implementation

Use naming conventions and strong types to make it easier to spot when sensitive data is being used. When creating structures, objects, or other complex entities, separate the sensitive and non-sensitive data as much as possible.

This makes it easier to spot places in the code where data is being used that is unencrypted.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	310	Cryptographic Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	693	Protection Mechanism Failure	**Research Concepts (primary)1000**
ChildOf	Category	719	OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	720	OWASP Top Ten 2007 Category A9 - Insecure Communications	Weaknesses in OWASP Top Ten (2007)629
ChildOf	Category	729	OWASP Top Ten 2004 Category A8 - Insecure Storage	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Base	312	Cleartext Storage of Sensitive Information	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	319	Cleartext Transmission of Sensitive Information	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	**Development Concepts (primary)699** **Research Concepts (primary)1000**
PeerOf	Weakness Base	327	Use of a Broken or Risky Cryptographic Algorithm	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Failure to encrypt data
OWASP Top Ten 2007	A8	CWE More Specific	Insecure Cryptographic Storage
OWASP Top Ten 2007	A9	CWE More Specific	Insecure Communications
OWASP Top Ten 2004	A8	CWE More Specific	Insecure Storage
WASC	4		Insufficient Transport Layer Protection

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
31	Accessing/Intercepting/Modifying HTTP Cookies	
37	Lifting Data Embedded in Client Distributions	
65	Passively Sniff and Capture Application Code Bound for Authorized Client	
117	Data Interception Attacks	
155	Screen Temporary Files for Sensitive Information	
157	Sniffing Attacks	
167	Lifting Sensitive Data from the Client	
204	Lifting cached, sensitive data embedded in client distributions (thick or thin)	
205	Lifting credential(s)/key material embedded in client distributions (thick or thin)	
258	Passively Sniffing and Capturing Application Code Bound for an Authorized Client During Dynamic Update	
259	Passively Sniffing and Capturing Application Code Bound for an Authorized Client During Patching	
260	Passively Sniffing and Capturing Application Code Bound for an Authorized Client During Initial Distribution	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 9, "Protecting Secret Data" Page 299. 2nd Edition. Microsoft. 2002.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 17: Failure to Protect Stored Data." Page 253. McGraw-Hill. 2010.

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		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Common Consequences, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Description, Detection Factors, Likelihood of Exploit, Name, Observed Examples, Potential Mitigations, References, Related Attack Patterns, Relationships, Taxonomy Mappings, Time of Introduction		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Failure to Encrypt Data
2010-02-16	Failure to Encrypt Sensitive Data

BACK TO TOP

Improper Certificate Validation

Risk

What might happen

Server certificate validation is explicitly disabled. This may be a not-removed by a debug statement. This enables the attacker to impersonate the server you are communicating with.

Cause

How does it happen

The application asks the user for their username and password and sends them to the server for validation. The application uses encrypted TLS/SSL connection. An attacker uses network monitoring tool to detect the IP of the server, then configures the local router to redirect all traffic with this IP to his own malicious server. The attacker sets a self-signed certificate on the malicious server. The TLS/SSL connection is terminated at the malicious server and the username and password is decrypted. The attacker steals the username and passwords.

General Recommendations

How to avoid it

1. If using an NSURLConnection, remove the connection:canAuthenticateAgainstProtectionSpace: and connection:didReceiveAuthenticationChallenge: methods from your NSURLConnectionDelegate. 2. If using AFNetworking, set the allowInvalidCertificates property to NO, which is the default.

Source Code Examples

Objc

Enable the server certificate validation in NSURLConnection class. Comment out the disabling methods, as shown in the example:

```
/*
// This code disables the server certificate validation, remove after debug
- (BOOL)connection:(NSURLConnection *)connection
canAuthenticateAgainstProtectionSpace:(NSURLProtectionSpace *)protectionSpace
{
return [protectionSpace.authenticationMethodisEqualToString:NSURLAuthenticationMethodServerTrust];
}

- (void)connection:(NSURLConnection *)connection
didReceiveAuthenticationChallenge:(NSURLAuthenticationChallenge *)challenge
{

[challenge.senderuseCredential:[NSURLCredentialcredentialForTrust:challenge.protectionSpace.serverTrust
forAuthenticationChallenge:challenge];
}
*/
```

Enabling the server certificate validation in AFNetworking class:

```
[[AFSecurityPolicydefaultPolicy] setAllowInvalidCertificates:false]
```

Screen Caching

Risk

What might happen

An attacker could get access to the application screenshots that were saved by the system. If sensitive data was presented in the screenshot, it could be leaked.

Cause

How does it happen

The application shows some sensitive data on a screen, such as a credit card numbers, using a regular UI element. The user presses the home button and sends the active application to the background. At the same moment, the system takes a screenshot of the application screen and saves the screenshot in a system folder. The screenshot is later used in an App Switcher to present open application screen previews. An attacker steals the mobile device, gets access to the screenshots folder, and steals the sensitive information.

General Recommendations

How to avoid it

1. Mark UITextView and UITextField that contain sensitive data as secure by setting the secureTextEntry property to YES. -Or- 2. Make the sensitive UI elements invisible just before the application moves to the background, and the screenshot is taken. To accomplish this, listen to UIApplicationDidEnterBackgroundNotification or implement an applicationDidEnterBackground: method in UIApplicationDelegate, and hide the sensitive UI element in this method.

Source Code Examples

Objc

Marking a UITextField as secure:

```
UITextField* textField = [[UITextFieldalloc] init];
textField.secureTextEntry = YES;
```

The example below shows how to hide a sensitive UI element just before the application goes to background:

```
- (void)viewDidLoad
{

    [[NSNotificationCenterdefaultCenter] addObserver:self
                                selector:@selector(didEnterBackground:)
                        name:UIApplicationDidEnterBackgroundNotification
                        object:nil];

    [[NSNotificationCenterdefaultCenter] addObserver:self
selector:@selector(didBecomeActive:)
name:UIApplicationDidBecomeActiveNotification
```

```
object:nil];

}

-(void)didEnterBackground:(NSNotification *)notification
{
    [self.creditCardNumberTextFieldsetHidden:YES];
}

-(void)didBecomeActive:(NSNotification *)notification
{
    [self.creditCardNumberTextFieldsetHidden:NO];
}
```

External Control of File Name or Path

Weakness ID: 73 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software allows user input to control or influence paths or file names that are used in filesystem operations.

Extended Description

This could allow an attacker to access or modify system files or other files that are critical to the application.

Path manipulation errors occur when the following two conditions are met:

1. An attacker can specify a path used in an operation on the filesystem.

2. By specifying the resource, the attacker gains a capability that would not otherwise be permitted.

For example, the program may give the attacker the ability to overwrite the specified file or run with a configuration controlled by the attacker.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

All

Operating Systems

UNIX: *(Often)*

Windows: *(Often)*

Mac OS: *(Often)*

Common Consequences

Scope	Effect
Confidentiality	The application can operate on unexpected files. Confidentiality is violated when the targeted filename is not directly readable by the attacker.
Integrity	The application can operate on unexpected files. This may violate integrity if the filename is written to, or if the filename is for a program or other form of executable code.
Availability	The application can operate on unexpected files. Availability can be violated if the attacker specifies an unexpected file that the application modifies. Availability can also be affected if the attacker specifies a filename for a large file, or points to a special device or a file that does not have the format that the application expects.

Likelihood of Exploit

High to Very High

Detection Methods

Automated Static Analysis

The external control or influence of filenames can often be detected using automated static analysis that models data flow within the software.

Automated static analysis might not be able to recognize when proper input validation is being performed, leading to false positives - i.e., warnings that do not have any security consequences or require any code changes.

Demonstrative Examples

Example 1

The following code uses input from an HTTP request to create a file name. The

programmer has not considered the possibility that an attacker could provide a file name such as "../../tomcat/conf/server.xml", which causes the application to delete one of its own configuration files (CWE-22).

(Bad Code)

Example Language: **Java**

```
String rName = request.getParameter("reportName");
File rFile = new File("/usr/local/apfr/reports/" + rName);
...
rFile.delete();
```

Example 2

The following code uses input from a configuration file to determine which file to open and echo back to the user. If the program runs with privileges and malicious users can change the configuration file, they can use the program to read any file on the system that ends with the extension .txt.

(Bad Code)

Example Language: **Java**

```
fis = new FileInputStream(cfg.getProperty("sub")+".txt");
amt = fis.read(arr);
out.println(arr);
```

Observed Examples

Reference	Description
CVE-2008-5748	Chain: external control of values for user's desired language and theme enables path traversal.
CVE-2008-5764	Chain: external control of user's target language enables remote file inclusion.

Potential Mitigations

Phase: Architecture and Design

When the set of filenames is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames, and reject all other inputs. For example, ID 1 could map to "inbox.txt" and ID 2 could map to "profile.txt". Features such as the ESAPI AccessReferenceMap provide this capability.

Phases: Architecture and Design; Operation

Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict all access to files within a particular directory.

Examples include the Unix chroot jail and AppArmor. In general, managed code may provide some protection.

This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.

Be careful to avoid CWE-243 and other weaknesses related to jails.

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.

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."

For filenames, use stringent whitelists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses such as CWE-23, and exclude directory separators such as "/" to avoid CWE-36. Use a whitelist of allowable file extensions, which will help to avoid CWE-434.

Phase: Implementation

Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences and symbolic links (CWE-23, CWE-59).

Phases: Installation; Operation

Use OS-level permissions and run as a low-privileged user to limit the scope of any successful attack.

Phases: Operation; Implementation

If you are using PHP, configure your application so that it does not use register_globals. During implementation, develop your application so that it does not rely on this feature, but be wary of implementing a register_globals emulation that is subject to weaknesses such as CWE-95, CWE-621, and similar issues.

Phase: Testing

Use automated static analysis tools that target this type of weakness. Many modern techniques use data flow analysis to minimize the number of false positives. This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Phase: Testing

Use 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.

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.

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	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	610	Externally Controlled Reference to a Resource in Another Sphere	Research Concepts1000
ChildOf	Weakness Class	642	External Control of Critical State Data	**Research Concepts (primary)1000**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	752	2009 Top 25 - Risky Resource Management	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
CanPrecede	Weakness Class	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Research Concepts1000
CanPrecede	Weakness Base	41	Improper Resolution of Path Equivalence	Research Concepts1000
CanPrecede	Weakness Base	59	Improper Link Resolution Before File Access ('Link Following')	Research Concepts1000
CanPrecede	Weakness Base	98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion')	Research Concepts1000
CanPrecede	Weakness Base	434	Unrestricted Upload of File with Dangerous Type	Research Concepts1000
CanAlsoBe	Weakness Base	99	Improper Control of Resource Identifiers ('Resource Injection')	Research Concepts1000

Relationship Notes

The external control of filenames can be the primary link in chains with other file-related weaknesses, as seen in the CanPrecede relationships. This is because software systems use files for many different purposes: to execute programs, load code libraries, to store application data, to store configuration settings, record temporary data, act as signals or semaphores to other processes, etc.

However, those weaknesses do not always require external control. For example, link-following weaknesses (CWE-59) often involve pathnames that are not controllable by the attacker at all.

The external control can be resultant from other issues. For example, in PHP applications, the register_globals setting can allow an attacker to modify variables that the programmer thought were immutable, enabling file inclusion (CWE-98) and path traversal (CWE-22). Operating with excessive privileges (CWE-250) might allow an attacker to specify an input filename that is not directly readable by the attacker, but is accessible to the privileged program. A buffer overflow (CWE-119) might give an attacker control over nearby memory locations that are related to pathnames, but were not directly modifiable by the attacker.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Path Manipulation

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
13	Subverting Environment Variable Values	
64	Using Slashes and URL Encoding Combined to Bypass Validation Logic	
72	URL Encoding	
78	Using Escaped Slashes in Alternate Encoding	
79	Using Slashes in Alternate Encoding	
76	Manipulating Input to File System Calls	
80	Using UTF-8 Encoding to Bypass Validation Logic	

References

"OWASP Enterprise Security API (ESAPI) Project". <http://www.owasp.org/index.php/ESAPI>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-09-08	CWE Content Team updated Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities	MITRE	Internal
2009-01-12	CWE Content Team updated Applicable Platforms, Causal Nature, Common Consequences, Demonstrative Examples, Description, Observed Examples, Other Notes, Potential Mitigations, References, Relationship Notes, Relationships, Weakness Ordinalities	MITRE	Internal
2009-03-10	CWE Content Team updated Potential Mitigations, Relationships	MITRE	Internal
2009-07-27	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2009-10-29	CWE Content Team updated Common Consequences, Description	MITRE	Internal
2009-12-28	CWE Content Team updated Detection Factors	MITRE	Internal
2010-02-16	CWE Content Team updated Potential Mitigations	MITRE	Internal

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Path Manipulation

BACK TO TOP

Privacy Violation

Weakness ID: 359 *(Weakness Class)* **Status:** Incomplete

Description

Description Summary

Mishandling private information, such as customer passwords or social security numbers, can compromise user privacy and is often illegal.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code contains a logging statement that tracks the contents of records added to a database by storing them in a log file. Among other values that are stored, the getPassword() function returns the user-supplied plaintext password associated with the account.

(Bad Code)

Example Language: **C#**

```
pass = GetPassword();
...
dbmsLog.WriteLine(id + ":" + pass + ":" + type + ":" + tstamp);
```

The code in the example above logs a plaintext password to the filesystem. Although many developers trust the filesystem as a safe storage location for data, it should not be trusted implicitly, particularly when privacy is a concern.

Other Notes

Privacy violations occur when: 1. Private user information enters the program. 2. The data is written to an external location, such as the console, file system, or network.

Private data can enter a program in a variety of ways:

- Directly from the user in the form of a password or personal information
- Accessed from a database or other data store by the application
- Indirectly from a partner or other third party

Sometimes data that is not labeled as private can have a privacy implication in a different context. For example, student identification numbers are usually not considered private because there is no explicit and publicly-available mapping to an individual student's personal information. However, if a school generates identification numbers based on student social security numbers, then the identification numbers should be considered private.

Security and privacy concerns often seem to compete with each other. From a security perspective, you should record all important operations so that any anomalous activity can later be identified. However, when private data is involved, this practice can in fact create risk. Although there are many ways in which private data can be handled unsafely, a common risk stems from misplaced trust. Programmers often trust the operating environment in which a program runs, and therefore believe that it is acceptable store private information on the file system, in the registry, or in other locally-controlled resources. However, even if access to certain resources is restricted, this does not guarantee that the individuals who do have access can be trusted.

For example, in 2004, an unscrupulous employee at AOL sold approximately 92 million private customer e-mail addresses to a spammer marketing an offshore gambling web site. In response to such high-profile exploits, the collection and management of private data is becoming increasingly regulated. Depending on its location, the type of business it conducts, and the nature of any private data it handles, an organization may be required to comply with one or more of the following federal and state regulations: - Safe Harbor Privacy Framework [REF-2] - Gramm-Leach Bliley Act (GLBA) [REF-3] - Health Insurance Portability and Accountability Act (HIPAA) [REF-4] - California SB-1386 [REF-5]

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	200	Information Exposure	**Research Concepts (primary)1000**

ChildOf	Category	254	Security Features	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	202	Privacy Leak through Data Queries	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Privacy Violation

References

J. Oates. "AOL man pleads guilty to selling 92m email addies". The Register. 2005. <http://www.theregister.co.uk/2005/02/07/aol_email_theft/>.

[REF-2] U.S. Department of Commerce. "Safe Harbor Privacy Framework". <http://www.export.gov/safeharbor/>.

[REF-3] Federal Trade Commission. "Financial Privacy: The Gramm-Leach Bliley Act (GLBA)". <http://www.ftc.gov/privacy/glbact/index.html>.

[REF-4] U.S. Department of Human Services. "Health Insurance Portability and Accountability Act (HIPAA)". <http://www.hhs.gov/ocr/hipaa/>.

[REF-5] Government of the State of California. "California SB-1386". 2002. <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html>.

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 Other Notes		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Other Notes, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Other Notes, References		

BACK TO TOP

Reversible One-Way Hash

Weakness ID: 328 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses a hashing algorithm that produces a hash value that can be used to determine the original input, or to find an input that can produce the same hash, more efficiently than brute force techniques.

Extended Description

This weakness is especially dangerous when the hash is used in security algorithms that require the one-way property to hold. For example, if an authentication system takes an incoming password and generates a hash, then compares the hash to another hash that it has stored in its authentication database, then the ability to create a collision could allow an attacker to provide an alternate password that produces the same target hash, bypassing authentication.

Time of Introduction

- Architecture and Design

Applicable Platforms

Languages

All

Observed Examples

Reference	Description
CVE-2006-4068	Hard-coded hashed values for username and password contained in client-side script, allowing brute-force offline attacks.

Potential Mitigations

Use a hash algorithm that is currently considered to be strong by experts in the field. MD-4 and MD-5 have known weaknesses. SHA-1 has also been broken.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	310	Cryptographic Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	326	Inadequate Encryption Strength	Research Concepts1000
ChildOf	Weakness Base	327	Use of a Broken or Risky Cryptographic Algorithm	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Reversible One-Way Hash

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
68	Subvert Code-signing Facilities	

References

Alexander Sotirov et al.. "MD5 considered harmful today". <http://www.phreedom.org/research/rogue-ca/>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Observed Example, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, References		

2009-10-29	CWE Content Team updated Relationships	MITRE	Internal

BACK TO TOP

Use of Hard-coded Password

Weakness ID: 259 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software contains a hard-coded password, which it uses for its own inbound authentication or for outbound communication to external components.

Extended Description

A hard-coded password typically leads to a significant authentication failure that can be difficult for the system administrator to detect. Once detected, it can be difficult to fix, so the administrator may be forced into disabling the product entirely. There are two main variations:

Inbound: the software contains an authentication mechanism that checks for a hard-coded password.

Outbound: the software connects to another system or component, and it contains hard-coded password for connecting to that component.

In the Inbound variant, a default administration account is created, and a simple password is hard-coded into the product and associated with that account. This hard-coded password is the same for each installation of the product, and it usually cannot be changed or disabled by system administrators without manually modifying the program, or otherwise patching the software. If the password is ever discovered or published (a common occurrence on the Internet), then anybody with knowledge of this password can access the product. Finally, since all installations of the software will have the same password, even across different organizations, this enables massive attacks such as worms to take place.

The Outbound variant applies to front-end systems that authenticate with a back-end service. The back-end service may require a fixed password which can be easily discovered. The programmer may simply hard-code those back-end credentials into the front-end software. Any user of that program may be able to extract the password. Client-side systems with hard-coded passwords pose even more of a threat, since the extraction of a password from a binary is usually very simple.

Time of Introduction

- Implementation
- Architecture and Design

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Authentication	If hard-coded passwords are used, it is almost certain that malicious users will gain access through the account in question.

Likelihood of Exploit

Very High

Detection Methods

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.

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Demonstrative Examples

Example 1

The following code uses a hard-coded password to connect to a database:

(Bad Code)

Example Language: **Java**

```
...
DriverManager.getConnection(url, "scott", "tiger");
...
```

This is an example of an external hard-coded password on the client-side of a connection. This code will run successfully, but anyone who has access to it will have access to the password. Once the program has shipped, there is no going back from the database user "scott" with a password of "tiger" unless the program is patched. A devious employee with access to this information can use it to break into the system. Even worse, if attackers have access to the bytecode for application, they can use the javap -c command to access the disassembled code, which will contain the values of the passwords used. The result of this operation might look something like the following for the example above:

(Attack)

```
javap -c ConnMngr.class
22: ldc #36; //String jdbc:mysql://ixne.com/rxsql
24: ldc #38; //String scott
26: ldc #17; //String tiger
```

Example 2

The following code is an example of an internal hard-coded password in the back-end:

(Bad Code)

Example Languages: **C and C++**

```
int VerifyAdmin(char *password) {
if (strcmp(password, "Mew!")) {

printf("Incorrect Password!\n");
return(0)
}
printf("Entering Diagnostic Mode...\n");
return(1);
}
```

(Bad Code)

Example Language: **Java**

```
int VerifyAdmin(String password) {
if (passwd.Equals("Mew!")) {
return(0)
}
//Diagnostic Mode
return(1);
}
```

Every instance of this program can be placed into diagnostic mode with the same password. Even worse is the fact that if this program is distributed as a binary-only distribution, it is very difficult to change that password or disable this "functionality."

Potential Mitigations

Phase: Architecture and Design

For outbound authentication: store passwords outside of the code in a strongly-protected, encrypted configuration file or database that is protected from access by all outsiders, including other local users on the same system. Properly protect the key (CWE-320). If you cannot use encryption to protect the file, then make sure that the permissions are as restrictive as possible.

Phase: Architecture and Design

For inbound authentication: Rather than hard-code a default username and password for first time logins, utilize a "first login" mode that requires the user to enter a unique strong password.

Phase: Architecture and Design

Perform access control checks and limit which entities can access the feature that requires the hard-coded password. For example, a feature might only be enabled through the system console instead of through a network connection.

Phase: Architecture and Design

For inbound authentication: apply strong one-way hashes to your passwords and store those hashes in a configuration file or database with appropriate access control. That way, theft of the file/database still requires the attacker to try to crack the password. When handling an incoming password during authentication, take the hash of the password and compare it to the hash that you have saved.

Use randomly assigned salts for each separate hash that you generate. This increases the amount of computation that an attacker needs to conduct a brute-force attack, possibly limiting the effectiveness of the rainbow table method.

Phase: Architecture and Design

For front-end to back-end connections: Three solutions are possible, although none are complete.

The first suggestion involves the use of generated passwords which are changed automatically and must be entered at given time intervals by a system administrator. These passwords will be held in memory and only be valid for the time intervals.

Next, the passwords used should be limited at the back end to only performing actions valid for the front end, as opposed to having full access.

Finally, the messages sent should be tagged and checksummed with time sensitive values so as to prevent replay style attacks.

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 perform a login. Using disassembled code, look at the associated instructions and see if any of them appear to be comparing the input to a fixed string or value.

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	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	344	Use of Invariant Value in Dynamically Changing Context	Research Concepts1000
ChildOf	Weakness Class	671	Lack of Administrator Control over Security	Research Concepts1000
ChildOf	Category	724	OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management	**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	Weakness Base	798	Use of Hard-coded Credentials	**Development Concepts (primary)699 Research Concepts (primary)1000**
PeerOf	Weakness Base	257	Storing Passwords in a Recoverable Format	Research Concepts1000
PeerOf	Weakness Base	321	Use of Hard-coded Cryptographic Key	Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Base	656	Reliance on Security through Obscurity	Research Concepts1000

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Password Management: Hard-Coded Password
CLASP			Use of hard-coded password
OWASP Top Ten 2004	A3	CWE More Specific	Broken Authentication and Session Management

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
188	Reverse Engineering	
189	Software Reverse Engineering	
190	Reverse Engineer an Executable to Expose Assumed Hidden Functionality or Content	
191	Read Sensitive Stings Within an Executable	
192	Protocol Reverse Engineering	
205	Lifting credential(s)/key material embedded in client distributions (thick or thin)	

White Box Definitions

Definition: A weakness where code path has:

1. end statement that passes a data item to a password function
2. value of the data item is a constant

Maintenance Notes

This entry should probably be split into multiple variants: an inbound variant (as seen in the second demonstrative example) and an outbound variant (as seen in the first demonstrative example). These variants are likely to have different consequences, detectability, etc. See extended description.

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		
2008-08-01		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 Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description, Potential Mitigations		
2008-11-13	CWE Content Team	MITRE	Internal
	Significant description modifications to emphasize different variants.		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Maintenance Notes, Other Notes, Potential Mitigations		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Maintenance Notes, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Related Attack Patterns, White Box Definitions		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Detection Factors, Name, Potential Mitigations, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Applicable Platforms		

Previous Entry Names

Change Date	Previous Entry Name
2010-02-16	Hard-Coded Password

BACK TO TOP

Improper Resource Shutdown or Release

Weakness ID: 404 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The program does not release or incorrectly releases a resource before it is made available for re-use.

Extended Description

When a resource is created or allocated, the developer is responsible for properly releasing the resource as well as accounting for all potential paths of expiration or invalidation, such as a set period of time or revocation.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Availability	Most unreleased resource issues result in general software reliability problems, but if an attacker can intentionally trigger a resource leak, the attacker might be able to launch a denial of service attack by depleting the resource pool.
Confidentiality	When a resource containing sensitive information is not correctly shutdown, it may expose the sensitive data in a subsequent allocation.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following method never closes the file handle it opens. The Finalize() method for StreamReader eventually calls Close(), but there is no guarantee as to how long it will take before the Finalize() method is invoked. In fact, there is no guarantee that Finalize() will ever be invoked. In a busy environment, this can result in the VM using up all of its available file handles.

(Bad Code)

Example Language: **Java**

```
private void processFile(string fName) {
StreamWriter sw = new
StreamWriter(fName);
string line;
while ((line = sr.ReadLine()) != null)
processLine(line);
}
```

Example 2

If an exception occurs after establishing the database connection and before the same connection closes, the pool of database connections may become exhausted. If the number of available connections is exceeded, other users cannot access this resource, effectively denying access to the application. Using the following database connection pattern will ensure that all opened connections are closed. The con.close() call should be the first executable statement in the finally block.

(Bad Code)

Example Language: **Java**

```
try {
Connection con = DriverManager.getConnection(some_connection_string)
}
catch ( Exception e ) {
log( e )
}
finally {

con.close()
}
```

Example 3

Under normal conditions the following C# code executes a database query, processes the results returned by the database, and closes the allocated SqlConnection object. But if an exception occurs while executing the SQL or processing the results, the SqlConnection object is not closed. If this happens often enough, the database will run out of available cursors and not be able to execute any more SQL queries.

(Bad Code)

Example Language: **C#**

```
...
SqlConnection conn = new SqlConnection(connString);
SqlCommand cmd = new SqlCommand(queryString);
cmd.Connection = conn;
conn.Open();
SqlDataReader rdr = cmd.ExecuteReader();
HarvestResults(rdr);
conn.Connection.Close();
...
```

Example 4

The following C function does not close the file handle it opens if an error occurs. If the process is long-lived, the process can run out of file handles.

(Bad Code)

Example Language: **C**

```
int decodeFile(char* fName) {
char buf[BUF_SZ];
FILE* f = fopen(fName, "r");
if (!f) {
printf("cannot open %s\n", fName);
return DECODE_FAIL;
}
else {
while (fgets(buf, BUF_SZ, f)) {
if (!checkChecksum(buf)) {
return DECODE_FAIL;
}
else {
decodeBlock(buf);
}
}
}
fclose(f);
return DECODE_SUCCESS;
}
```

Example 5

In this example, the program fails to use matching functions such as malloc/free, new/delete, and new[]/delete[] to allocate/deallocate the resource.

(Bad Code)

Example Language: **C++**

```
class A {
void foo();
```

```
};
void A::foo(){
int *ptr;
ptr = (int*)malloc(sizeof(int));
delete ptr;
}
```

Example 6

In this example, the program calls the delete[] function on non-heap memory.

(Bad Code)

Example Language: **C++**

```
class A{
void foo(bool);
};
void A::foo(bool heap) {
int localArray[2] = {
11,22
};
int *p = localArray;
if (heap){
p = new int[2];
}
delete[] p;
}
```

Observed Examples

Reference	Description
CVE-1999-1127	Does not shut down named pipe connections if malformed data is sent.
CVE-2001-0830	Sockets not properly closed when attacker repeatedly connects and disconnects from server.
CVE-2002-1372	Return values of file/socket operations not checked, allowing resultant consumption of file descriptors.

Potential Mitigations

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate resource-shutdown weaknesses.

For example, languages such as Java, Ruby, and Lisp perform automatic garbage collection that releases memory for objects that have been deallocated.

Phase: Implementation

It is good practice to be responsible for freeing all resources you allocate and to be consistent with how and where you free memory in a function. If you allocate memory that you intend to free upon completion of the function, you must be sure to free the memory at all exit points for that function including error conditions.

Phase: Implementation

Memory should be allocated/freed using matching functions such as malloc/free, new/delete, and new[]/delete[].

Phase: Implementation

When releasing a complex object or structure, ensure that you properly dispose of all of its member components, not just the object itself.

Phase: Testing

Use 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.

Phase: Testing

Stress-test the software by calling it simultaneously from a large number of threads or processes, and look for evidence of any unexpected behavior. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Phase: Testing

Identify error conditions that are not likely to occur during normal usage and trigger them. For example, run the program under low memory conditions, run with insufficient privileges or permissions, interrupt a transaction before it is completed, or disable

connectivity to basic network services such as DNS. Monitor the software for any unexpected behavior. If you trigger an unhandled exception or similar error that was discovered and handled by the application's environment, it may still indicate unexpected conditions that were not handled by the application itself.

Weakness Ordinalities

Ordinality	Description
Primary	Failing to properly release or shutdown resources can be primary to resource exhaustion, performance, and information confidentiality problems to name a few.
Resultant	Failing to properly release or shutdown resources can be resultant from improper error handling or insufficient resource tracking.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Weakness Class	664	Improper Control of a Resource Through its Lifetime	**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	743	CERT C Secure Coding Section 09 - Input Output (FIO)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	752	2009 Top 25 - Risky Resource Management	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
PeerOf	Weakness Class	405	Asymmetric Resource Consumption (Amplification)	Research Concepts1000
ParentOf	Weakness Variant	262	Not Using Password Aging	**Research Concepts (primary)1000**
ParentOf	Weakness Base	263	Password Aging with Long Expiration	**Research Concepts (primary)1000**
ParentOf	Weakness Base	299	Improper Check for Certificate Revocation	**Research Concepts (primary)1000**
ParentOf	Weakness Base	459	Incomplete Cleanup	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	568	finalize() Method Without super.finalize()	**Research Concepts (primary)1000**
ParentOf	Weakness Base	619	Dangling Database Cursor ('Cursor Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	763	Release of Invalid Pointer or Reference	**Research Concepts (primary)1000**
ParentOf	Weakness Base	772	Missing Release of Resource after Effective Lifetime	**Research Concepts (primary)1000**
PeerOf	Weakness Base	239	Failure to Handle Incomplete Element	Research Concepts1000

Relationship Notes

Overlaps memory leaks, asymmetric resource consumption, malformed input errors.

Functional Areas

- Non-specific

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Improper resource shutdown or release
7 Pernicious Kingdoms			Unreleased Resource
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service
CERT C Secure Coding	FIO42-C		Ensure files are properly closed when they are no longer needed

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
118	Data Leakage Attacks	
119	Resource Depletion	
125	Resource Depletion through Flooding	
130	Resource Depletion through Allocation	

131	Resource Depletion through Leak

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-08-15	 Suggested OWASP Top Ten 2004 mapping	Veracode	External
2008-09-08	CWE Content Team updated Description, Relationships, Other Notes, Taxonomy Mappings	MITRE	Internal
2008-10-14	CWE Content Team updated Relationships	MITRE	Internal
2008-11-24	CWE Content Team updated Relationships, Taxonomy Mappings	MITRE	Internal
2009-01-12	CWE Content Team updated Common Consequences, Likelihood of Exploit, Other Notes, Potential Mitigations, Relationship Notes, Relationships, Weakness Ordinalities	MITRE	Internal
2009-03-10	CWE Content Team updated Potential Mitigations	MITRE	Internal
2009-05-27	CWE Content Team updated Description, Relationships	MITRE	Internal
2009-07-27	CWE Content Team updated Demonstrative Examples, Related Attack Patterns	MITRE	Internal
2009-10-29	CWE Content Team updated Other Notes	MITRE	Internal
2010-02-16	CWE Content Team updated Potential Mitigations, Relationships	MITRE	Internal

BACK TO TOP

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 Lifetime	**Research Concepts (primary)1000**
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 updated Time of Introduction	Cigital	External
2008-08-01	 added/updated white box definitions	KDM Analytics	External
2008-08-15	 Suggested OWASP Top Ten 2004 mapping	Veracode	External
2008-09-08	CWE Content Team updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes	MITRE	Internal
2008-10-14	CWE Content Team updated Description	MITRE	Internal
2009-03-10	CWE Content Team updated Other Notes	MITRE	Internal
2009-05-27	CWE Content Team updated Name	MITRE	Internal
2009-07-17	KDM Analytics Improved the White Box Definition		External
2009-07-27	CWE Content Team updated White Box Definitions	MITRE	Internal
2009-10-29	CWE Content Team updated Modes of Introduction, Other Notes	MITRE	Internal
2010-02-16	CWE Content Team updated Relationships	MITRE	Internal

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')

Unchecked Return Value

Weakness ID: 252 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not check the return value from a method or function, which can prevent it from detecting unexpected states and conditions.

Extended Description

Two common programmer assumptions are "this function call can never fail" and "it doesn't matter if this function call fails". If an attacker can force the function to fail or otherwise return a value that is not expected, then the subsequent program logic could lead to a vulnerability, because the software is not in a state that the programmer assumes. For example, if the program calls a function to drop privileges but does not check the return code to ensure that privileges were successfully dropped, then the program will continue to operate with the higher privileges.

Time of Introduction

- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Integrity	The data which were produced as a result of a function call could be in a bad state upon return. If the return value is not checked, then this bad data may be used in operations and lead to a crash or other unintended behaviors.

Likelihood of Exploit

Low

Demonstrative Examples

Example 1

Consider the following code segment:

(Bad Code)

Example Language: **C**

```
char buf[10], cp_buf[10];
fgets(buf, 10, stdin);
strcpy(cp_buf, buf);
```

The programmer expects that when fgets() returns, buf will contain a null-terminated string of length 9 or less. But if an I/O error occurs, fgets() will not null-terminate buf. Furthermore, if the end of the file is reached before any characters are read, fgets() returns without writing anything to buf. In both of these situations, fgets() signals that something unusual has happened by returning NULL, but in this code, the warning will not be noticed. The lack of a null terminator in buf can result in a buffer overflow in the subsequent call to strcpy().

Example 2

The following code does not check to see if memory allocation succeeded before attempting to use the pointer returned by malloc().

(Bad Code)

Example Language: **C**

```
buf = (char*) malloc(req_size);
strncpy(buf, xfer, req_size);
```

The traditional defense of this coding error is: "If my program runs out of memory, it will fail. It doesn't matter whether I handle the error or simply allow the program to die with a segmentation fault when it tries to dereference the null pointer." This argument ignores three important considerations:

- Depending upon the type and size of the application, it may be possible to free memory that is being used elsewhere so that execution can continue.
- It is impossible for the program to perform a graceful exit if required. If the program is performing an atomic operation, it can leave the system in an inconsistent state.
- The programmer has lost the opportunity to record diagnostic information. Did the call to malloc() fail because req_size was too large or because there were too many requests being handled at the same time? Or was it caused by a memory leak that has built up over time? Without handling the error, there is no way to know.

Example 3

The following code loops through a set of users, reading a private data file for each user. The programmer assumes that the files are always 1 kilobyte in size and therefore ignores the return value from Read(). If an attacker can create a smaller file, the program will recycle the remainder of the data from the previous user and handle it as though it belongs to the attacker.

(Bad Code)

Example Language: **Java**

```
char[] byteArray = new char[1024];
for (IEnumerator i=users.GetEnumerator(); i.MoveNext() ;i.Current()) {
String userName = (String) i.Current();
String pFileName = PFILE_ROOT + "/" + userName;
StreamReader sr = new StreamReader(pFileName);
sr.Read(byteArray,0,1024);//the file is always 1k bytes
sr.Close();
processPFile(userName, byteArray);
}
```

(Bad Code)

Example Language: **Java**

```
FileInputStream fis;
byte[] byteArray = new byte[1024];
for (Iterator i=users.iterator(); i.hasNext();) {
String userName = (String) i.next();
String pFileName = PFILE_ROOT + "/" + userName;
FileInputStream fis = new FileInputStream(pFileName);
fis.read(byteArray); // the file is always 1k bytes
fis.close();
processPFile(userName, byteArray);
```

Example 4

The following code does not check to see if the string returned by getParameter() is null before calling the member function compareTo(), potentially causing a NULL dereference.

(Bad Code)

Example Language: **Java**

```
String itemName = request.getParameter(ITEM_NAME);
if (itemName.compareTo(IMPORTANT_ITEM)) {
...
}
...
```

The following code does not check to see if the string returned by theItem property is null before calling the member function Equals(), potentially causing a NULL dereference. string itemName = request.Item(ITEM_NAME);

(Bad Code)

```
if (itemName.Equals(IMPORTANT_ITEM)) {
...
}
...
```

The traditional defense of this coding error is: "I know the requested value will always exist because.... If it does not exist, the program cannot perform the desired behavior so it doesn't matter whether I handle the error or simply allow the program to die dereferencing a null value." But attackers are skilled at finding unexpected paths through programs, particularly when exceptions are involved.

Example 5

The following code shows a system property that is set to null and later dereferenced by a programmer who mistakenly assumes it will always be defined.

(Bad Code)

```
System.clearProperty("os.name");
...
String os = System.getProperty("os.name");
if (os.equalsIgnoreCase("Windows 95")) System.out.println("Not supported");
```

The traditional defense of this coding error is: "I know the requested value will always exist because.... If it does not exist, the program cannot perform the desired behavior so it doesn't matter whether I handle the error or simply allow the program to die dereferencing a null value." But attackers are skilled at finding unexpected paths through programs, particularly when exceptions are involved.

Example 6

The following VB.NET code does not check to make sure that it has read 50 bytes from myfile.txt. This can cause DoDangerousOperation() to operate on an unexpected value.

(Bad Code)

```
Dim MyFile As New FileStream("myfile.txt", FileMode.Open, FileAccess.Read, FileShare.Read)
Dim MyArray(50) As Byte
MyFile.Read(MyArray, 0, 50)
DoDangerousOperation(MyArray(20))
```

In .NET, it is not uncommon for programmers to misunderstand Read() and related methods that are part of many System.IO classes. The stream and reader classes do not consider it to be unusual or exceptional if only a small amount of data becomes available. These classes simply add the small amount of data to the return buffer, and set the return value to the number of bytes or characters read. There is no guarantee that the amount of data returned is equal to the amount of data requested.

Example 7

It is not uncommon for Java programmers to misunderstand read() and related methods that are part of many java.io classes. Most errors and unusual events in Java result in an exception being thrown. But the stream and reader classes do not consider it unusual or exceptional if only a small amount of data becomes available. These classes simply add the small amount of data to the return buffer, and set the return value to the number of bytes or characters read. There is no guarantee that the amount of data returned is equal to the amount of data requested. This behavior makes it important for programmers to examine the return value from read() and other IO methods to ensure that they receive the amount of data they expect.

Example 8

This example takes an IP address from a user, verifies that it is well formed and then looks up the hostname and copies it into a buffer.

(Bad Code)

Example Language: **C**

```
void host_lookup(char *user_supplied_addr){
struct hostent *hp;
in_addr_t *addr;
char hostname[64];
in_addr_t inet_addr(const char *cp);

/*routine that ensures user_supplied_addr is in the right format for conversion */
validate_addr_form(user_supplied_addr);
addr = inet_addr(user_supplied_addr);
hp = gethostbyaddr( addr, sizeof(struct in_addr), AF_INET);
strcpy(hostname, hp->h_name);
}
```

If an attacker provides an address that appears to be well-formed, but the address does not resolve to a hostname, then the call to gethostbyaddr() will return NULL. When this occurs, a NULL pointer dereference (CWE-476) will occur in the call to strcpy().

Note that this example is also vulnerable to a buffer overflow (see CWE-119).

Observed Examples

Reference	Description
CVE-2007-3798	Unchecked return value leads to resultant integer overflow and code execution.
CVE-2006-4447	Program does not check return value when invoking functions to drop privileges, which could leave users with higher privileges than expected by forcing those functions to fail.
CVE-2006-2916	Program does not check return value when invoking functions to drop privileges, which could leave users with higher privileges than expected by forcing those functions to fail.

Potential Mitigations

Phase: Implementation

Check the results of all functions that return a value and verify that the value is expected.

Effectiveness: High

Checking the return value of the function will typically be sufficient, however beware of race conditions (CWE-362) in a concurrent environment.

Phase: Implementation

Ensure that you account for all possible return values from the function.

Phase: Implementation

When designing a function, make sure you return a value or throw an exception in case of an error.

Background Details

Many functions will return some value about the success of their actions. This will alert the program whether or not to handle any errors caused by that function.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to	Named Chain(s) this relationship pertains to
ChildOf	Weakness Class	227	Failure to Fulfill API Contract ('API Abuse')	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700**	
ChildOf	Category	389	Error Conditions, Return Values, Status Codes	Development Concepts699	
ChildOf	Category	728	OWASP Top Ten 2004 Category A7 - Improper Error Handling	**Weaknesses in OWASP Top Ten (2004) (primary)711**	
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**	
ChildOf	Weakness Class	754	Improper Check for Unusual or Exceptional Conditions	**Research Concepts (primary)1000**	
CanPrecede	Weakness Base	476	NULL Pointer Dereference	Research Concepts1000	Unchecked Return Value to NULL Pointer

					Dereference690
StartsChain	Compound Element: Chain	690	Unchecked Return Value to NULL Pointer Dereference	Named Chains709	Unchecked Return Value to NULL Pointer Dereference690
PeerOf	Weakness Base	273	Improper Check for Dropped Privileges	Research Concepts1000	

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Unchecked Return Value
CLASP			Ignored function return value
OWASP Top Ten 2004	A7	CWE More Specific	Improper Error Handling
CERT C Secure Coding	MEM32-C		Detect and handle memory allocation errors

References

[REF-7] Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 7, "Program Building Blocks" Page 341.. 1st Edition. Addison Wesley. 2006.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 20, "Checking Returns" Page 624. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-09-08	CWE Content Team updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings	MITRE	Internal
2008-11-24	CWE Content Team updated Relationships, Taxonomy Mappings	MITRE	Internal
2009-01-12	CWE Content Team updated Background Details, Demonstrative Examples, Description, Observed Examples, Other Notes, Potential Mitigations	MITRE	Internal
2009-03-10	CWE Content Team updated Relationships	MITRE	Internal
2009-05-27	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2009-07-27	CWE Content Team updated Demonstrative Examples	MITRE	Internal
2009-12-28	CWE Content Team updated Common Consequences, Demonstrative Examples, References	MITRE	Internal
2010-02-16	CWE Content Team updated Demonstrative Examples, Potential Mitigations, References	MITRE	Internal
2010-04-05	CWE Content Team updated Demonstrative Examples	MITRE	Internal

BACK TO TOP

Jailbrake File Referenced By Name

Risk

What might happen

In a jail-broken device, an attacker could manipulate the contents of a file written by the application. A buffer overflow or other unintended behavior may happen when the modified file is read back by the application. This may allow an attacker to seize control of the system.

Cause

How does it happen

The application creates a temporary file. An attacker detects a file creation event, deletes the created file, and creates a new file with the same name but different permissions. The application writes to a file referencing it by name. Data is written to the file owned by the attacker without the application noticing it. The attacker steals sensitive information from the temporary file or modifies its content. The application reads back the tampered file, and a buffer overflow or other unintended behavior happens. The attacker exploits the buffer overflow to gain control of the application. For more information see section “Files in Publicly Writable Directories Are Dangerous” in “Apple Secure Coding Guide” document: https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/

General Recommendations

How to avoid it

Reference all files by descriptor rather than by name.

Source Code Examples

Objc

Example of insecure way to reference files by name.

```
NSString* fileName = [NSTemporaryDirectory() stringByAppendingString:@"/f1.txt"];

NSString* stringToWrite = @"Hello world";
[stringToWrite writeToFile:fileName atomically:YES];
```

Example of secure way to reference files by descriptor.

```
NSString* fileNameTemplate = [NSTemporaryDirectory() stringByAppendingString:@"/myTmpFile-
XXXXXX.txt"];

const size_t bufLength = 2048;

char* fileNameBuf[bufLength];
strncpy(fileNameBuf, [fileNameTemplate cStringUsingEncoding:NSUTF8StringEncoding], bufLength);

int fileDescriptor = mkstemp(fileNameBuf);

NSFileHandle* fileHandle = [[NSFileHandle alloc] initWithFileDescriptor:fileDescriptor];


NSString* stringToWrite = @"Hello world";
[fileHandle writeData: [stringToWrite dataUsingEncoding:NSUTF8StringEncoding]];
```

Jailbreak Unchecked File Operation Result Code

Risk

What might happen

Data written to temporary file may become corrupted. A buffer overflow or other unintended behavior may happen when the corrupted file is read back by the application. This may allow an attacker to seize control of the system.

Cause

How does it happen

The application writes data to a temporary file. The write operation fails in the middle. Part of the data is written to the file, and another part is lost. The application does not check the result code of the file operation, and takes no corrective actions. The application reads back the corrupted file, and a buffer overflow or other unintended behavior happens. An attacker exploits the buffer overflow to gain control of the application. For more information see section “Check Result Codes” in “Apple Secure Coding Guide” document: https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/

General Recommendations

How to avoid it

Check the result code of every file operation and address failures appropriately.

Source Code Examples

Objc

Example of ignoring file operation result code (insecure).

```
NSString* stringToWrite = @"Hello world";
NSString* filePath = [NSTemporaryDirectory() stringByAppendingString:@"/f1.txt"];
[stringToWrite writeToFile:filePath atomically:NO];
```

Example of checking file operation result code (secure).

```
NSString* stringToWrite = @"Hello world";

NSString* filePath = [NSTemporaryDirectory() stringByAppendingString:@"/f1.txt"];

if (![stringToWrite writeToFile:filePath atomically:NO])
{
    [[NSException exceptionWithName:@"FileWriteError" reason:@"" userInfo:nil] raise];
};
```

Unchecked CString Convertion

Risk

What might happen

Converted C-String length may be less than the CFString length. If the program then makes decisions based on that erroneously converted string, any number of erroneous behaviors can result.

Cause

How does it happen

A CFString have an explicit length and can contain null bytes at arbitrary locations in the data. A CFString with a null character in the middle is converted into C-String. The resulting C-String is evaluated. The application behaves incorrectly behavior because the resulting C string effectively ends at the first null byte. Example of a real life attack: This vulnerability occurred in many SSL stacks a few years ago. By applying for an SSL cert for a carefully crafted subdomain of a domain that you own, you could effectively create a certificate that was valid for arbitrary domains. Consider a subdomain in the form targetdomain.tld[null_byte].yourdomain.tld. Because the certificate signing request contains a Pascal string (which like CFString can contain null characters), assuming that the certificate authority interprets it correctly, the certificate authority would contact the owner of yourdomain.tld and would ask for permission to deliver the certificate. Because you own the domain, you would agree to it. You would then have a certificate that is valid for the rather odd-looking subdomain in question. When checking the certificate for validity, however, many SSL stacks incorrectly converted that Pascal string into a C string without any validity checks. When this happened, the resulting C string contained only the targetdomain.tld portion. The SSL stack then compared that truncated version with the domain the user requested, and interpreted the certificate as being valid for the targeted domain. In some cases, it was even possible to construct wildcard certificates that were valid for every possible domain in such browsers (*.com[null] .yourdomain.tld would match every .com address, for example). For more information see section “Avoiding Buffer Underflows” in “Apple Secure Coding Guide” document: https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/

General Recommendations

How to avoid it

1. Avoid converting non-C strings (CFStringRef objects, NSString objects, CFDataRef objects) into C strings if possible. Instead, work with the strings in their original format. 2. If this is not possible, always perform length checks on the resulting C string or check for null bytes in the source data.

Source Code Examples

Objc

Example of converting CFString to C-String without length check (insecure).

```
CFStringRef s1 = CFSTR("Hello");
```

```
size_t buf_len = 10;

char buffer[buf_len];

CFStringGetCString(s1,buffer,buf_len,kCFStringEncodingASCII);
```

Failure to Clear Heap Memory Before Release ('Heap Inspection')

Weakness ID: 244 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

Using realloc() to resize buffers that store sensitive information can leave the sensitive information exposed to attack, because it is not removed from memory.

Extended Description

When sensitive data such as a password or an encryption key is not removed from memory, it could be exposed to an attacker using a "heap inspection" attack that reads the sensitive data using memory dumps or other methods. The realloc() function is commonly used to increase the size of a block of allocated memory. This operation often requires copying the contents of the old memory block into a new and larger block. This operation leaves the contents of the original block intact but inaccessible to the program, preventing the program from being able to scrub sensitive data from memory. If an attacker can later examine the contents of a memory dump, the sensitive data could be exposed.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Confidentiality	Be careful using vfork() and fork() in security sensitive code. The process state will not be cleaned up and will contain traces of data from past use.

Demonstrative Examples

Example 1

The following code calls realloc() on a buffer containing sensitive data:

(Bad Code)

Example Language: **C**

```
cleartext_buffer = get_secret();...
cleartext_buffer = realloc(cleartext_buffer, 1024);
...
scrub_memory(cleartext_buffer, 1024);
```

There is an attempt to scrub the sensitive data from memory, but realloc() is used, so a copy of the data can still be exposed in the memory originally allocated for cleartext_buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	226	Sensitive Information Uncleared Before Release	**Research Concepts (primary)1000**
ChildOf	Weakness Class	227	Failure to Fulfill API Contract ('API Abuse')	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
CanPrecede	Weakness Class	669	Incorrect Resource Transfer Between Spheres	Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Heap Inspection
CERT C Secure Coding	MEM03-C		Clear sensitive information stored in reusable resources returned for reuse

White Box Definitions

A weakness where code path has:

1. start statement that stores information in a buffer
2. end statement that resize the buffer and
3. path does not contain statement that performs cleaning of the buffer

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Name, Relationships, Other Notes, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Relationships		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Other Notes		

Previous Entry Names	
Change Date	**Previous Entry Name**
2008-04-11	Heap Inspection
2008-09-09	Failure to Clear Heap Memory Before Release
2009-05-27	Failure to Clear Heap Memory Before Release (aka 'Heap Inspection')

BACK TO TOP

Buffer Size Literal Condition

Risk

What might happen

An attacker can exploit the buffer overflow to execute an arbitrary code with the privileges of the vulnerable application.

Cause

How does it happen

Buffer size is specified by a number literal, and access to the buffer is checked using number literal. A developer makes changes to the code, and reduces the allocated buffer size, but forgets to reduce the literal in conditional statement. A buffer overflow is created. At run time, the following scenario happens: The overflown buffer is allocated in stack. Right after the end of the buffer, the function return address is located. An attacker manipulates the input in such a way that when data is written into the buffer, the return address is overwritten. The new return address points to a memory segment under the attacker control. When the function returns, the attacker code is executed with the application privileges.

General Recommendations

How to avoid it

Define a constant that holds the buffer size, then use this constant throughout the code.

Source Code Examples

Objc

Code example that is vulnerable to buffer overflow after code changes.

```
void f() {
    char buf[10];
    char* sourceString = istream.read("input");
    if (strlen(sourceString) < 10)
    {
        strcpy(buf,sourceString);
    }
}
```

Code that is resilient to buffer overflow after code changes.

```
void f()
{
    const int MAX_INPUT_SIZE = 256;
    const int BUFFER_SIZE = 10;
    char buf[BUFFER_SIZE];
    char* sourceString = istream.read("input");
    if (strnlen(sourceString,MAX_INPUT_SIZE) < BUFFER_SIZE)
    {
        strcpy(buf,sourceString);
    }
}
```

Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')

Weakness ID: 89 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Extended Description

Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.

SQL injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

All

Technology Classes

Database-Server

Modes of Introduction

This weakness typically appears in data-rich applications that save user inputs in a database.

Common Consequences

Scope	Effect
Confidentiality	Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL injection vulnerabilities.
Authentication	If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.
Authorization	If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL injection vulnerability.
Integrity	Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL injection attack.

Likelihood of Exploit

Very High

Enabling Factors for Exploitation

The application dynamically generates queries that contain user input.

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 might not be able to recognize when proper input validation is being performed, leading to false positives - i.e., warnings that do not have any security consequences or do not require any code changes.

Automated static analysis might not be able to detect the usage of custom API functions or third-party libraries that indirectly invoke SQL commands, leading to false negatives - especially if the API/library code is not available for analysis.

Manual Analysis

Manual analysis can be useful for finding this weakness, but it might not achieve desired code coverage within limited time constraints. This becomes difficult for weaknesses that must be considered for all inputs, since the attack surface can be too large.

Demonstrative Examples

Example 1

In 2008, a large number of web servers were compromised using the same SQL injection attack string. This single string worked against many different programs. The SQL injection was then used to modify the web sites to serve malicious code. [1]

Example 2

The following code dynamically constructs and executes a SQL query that searches for items matching a specified name. The query restricts the items displayed to those where owner matches the user name of the currently-authenticated user.

(Bad Code)

Example Language: **C#**

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = '" + userName + "' AND itemname = '" + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

The query that this code intends to execute follows:

```
SELECT * FROM items WHERE owner = <userName> AND itemname = <itemName>;
```

However, because the query is constructed dynamically by concatenating a constant base query string and a user input string, the query only behaves correctly if itemName does not contain a single-quote character. If an attacker with the user name wiley enters the string:

(Attack)

```
name' OR 'a'='a
```

for itemName, then the query becomes the following:

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

The addition of the:

(Attack)

```
OR 'a'='a'
```

condition causes the WHERE clause to always evaluate to true, so the query becomes logically equivalent to the much simpler query:

(Attack)

```
SELECT * FROM items;
```

This simplification of the query allows the attacker to bypass the requirement that the query only return items owned by the authenticated user; the query now returns all entries stored in the items table, regardless of their specified owner.

Example 3

This example examines the effects of a different malicious value passed to the query constructed and executed in the previous example.

If an attacker with the user name wiley enters the string:

(Attack)

```
name'; DELETE FROM items; --
```

for itemName, then the query becomes the following two queries:

(Attack)

Example Language: **SQL**

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
--'
```

Many database servers, including Microsoft(R) SQL Server 2000, allow multiple SQL statements separated by semicolons to be executed at once. While this attack string results in an error on Oracle and other database servers that do not allow the batch-execution of statements separated by semicolons, on databases that do allow batch execution, this type of attack allows the attacker to execute arbitrary commands against the database.

Notice the trailing pair of hyphens (--), which specifies to most database servers that the remainder of the statement is to be treated as a comment and not executed. In this case the comment character serves to remove the trailing single-quote left over from the modified query. On a database where comments are not allowed to be used in this way, the general attack could still be made effective using a trick similar to the one shown in the previous example.

If an attacker enters the string

(Attack)

```
name'; DELETE FROM items; SELECT * FROM items WHERE 'a'='a
```

Then the following three valid statements will be created:

(Attack)

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name';
DELETE FROM items;
SELECT * FROM items WHERE 'a'='a';
```

One traditional approach to preventing SQL injection attacks is to handle them as an input validation problem and either accept only characters from a whitelist of safe values or identify and escape a blacklist of potentially malicious values. Whitelisting can be a very effective means of enforcing strict input validation rules, but parameterized SQL statements require less maintenance and can offer more guarantees with respect to security. As is almost always the case, blacklisting is riddled with loopholes that make it ineffective at preventing SQL injection attacks. For example, attackers can:

- Target fields that are not quoted
- Find ways to bypass the need for certain escaped meta-characters
- Use stored procedures to hide the injected meta-characters.

Manually escaping characters in input to SQL queries can help, but it will not make your application secure from SQL injection attacks.

Another solution commonly proposed for dealing with SQL injection attacks is to use stored procedures. Although stored procedures prevent some types of SQL injection attacks, they fail to protect against many others. For example, the following PL/SQL procedure is vulnerable to the same SQL injection attack shown in the first example.

(Bad Code)

```
procedure get_item ( itm_cv IN OUT ItmCurTyp, usr in varchar2, itm in varchar2)
is open itm_cv for
' SELECT * FROM items WHERE ' || 'owner = '|| usr || ' AND itemname = ' || itm || ';
end get_item;
```

Stored procedures typically help prevent SQL injection attacks by limiting the types of statements that can be passed to their parameters. However, there are many ways around the limitations and many interesting statements that can still be passed to stored procedures. Again, stored procedures can prevent some exploits, but they will not make your application secure against SQL injection attacks.

Example 4

MS SQL has a built in function that enables shell command execution. An SQL injection in such a context could be disastrous. For example, a query of the form:

(Bad Code)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='$user_input' ORDER BY PRICE
```

Where $user_input is taken from the user and unfiltered.

If the user provides the string:

(Attack)

```
' exec master..xp_cmdshell 'vol' --
```

The query will take the following form: "

(Attack)

```
SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY='' exec master..xp_cmdshell 'vol' --' ORDER BY PRICE
```

Now, this query can be broken down into:

- [1] a first SQL query: SELECT ITEM,PRICE FROM PRODUCT WHERE ITEM_CATEGORY=''
- [2] a second SQL query, which executes a shell command: exec master..xp_cmdshell 'vol'
- [3] an MS SQL comment: --' ORDER BY PRICE

As can be seen, the malicious input changes the semantics of the query into a query, a shell command execution and a comment.

Example 5

This code intends to print a message summary given the message ID.

(Bad Code)

Example Language: **PHP**

```
$id = $_COOKIE["mid"];
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

The programmer may have skipped any input validation on $id under the assumption that attackers cannot modify the cookie. However, this is easy to do with custom client code or even in the web browser.

While $id is wrapped in single quotes in the call to mysql_query(), an attacker could simply change the incoming mid cookie to:

(Attack)

```
1432' or '1' = '1
```

This would produce the resulting query:

(Result)

```
SELECT MessageID, Subject FROM messages WHERE MessageID = '1432' or '1' = '1'
```

Not only will this retrieve message number 1432, it will retrieve all other messages.

In this case, the programmer could apply a simple modification to the code to eliminate the SQL injection:

(Good Code)

Example Language: **PHP**

```
$id = intval($_COOKIE["mid"]);
mysql_query("SELECT MessageID, Subject FROM messages WHERE MessageID = '$id'");
```

However, if this code is intended to support multiple users with different message boxes, the code might also need an access control check (CWE-285) to ensure that the application user has the permission to see that message.

Example 6

This example attempts to take a last name provided by a user and enter it into a database.

(Bad Code)

Example Language: **Perl**

```
$userKey = getUserID();
$name = getUserInput();
# ensure only letters, hyphens and apostrophe are allowed
$name = whiteList($name, "^a-zA-z'-$");
$query = "INSERT INTO last_names VALUES('$userKey', '$name')";
```

While the programmer applies a whitelist to the user input, it has shortcomings. First of all, the user is still allowed to provide hyphens which are used as comment structures in SQL. If a user specifies -- then the remainder of the statement will be treated as a comment, which may bypass security logic. Furthermore, the whitelist permits the apostrophe which is also a data / command separator in SQL. If a user supplies a name with an apostrophe, they may be able to alter the structure of the whole statement and even change control flow of the program, possibly accessing or modifying confidential information. In this situation, both the hyphen and apostrophe are legitimate characters for a last name and permitting them is required. Instead, a programmer may want to use a prepared statement or apply an encoding routine to the input to prevent any data / directive misinterpretations.

Observed Examples

Reference	Description
CVE-2004-0366	chain: SQL injection in library intended for database authentication allows SQL injection and authentication bypass.
CVE-2008-2790	SQL injection through an ID that was supposed to be numeric.
CVE-2008-2223	SQL injection through an ID that was supposed to be numeric.
CVE-2007-6602	SQL injection via user name.
CVE-2008-5817	SQL injection via user name or password fields.
CVE-2003-0377	SQL injection in security product, using a crafted group name.
CVE-2008-2380	SQL injection in authentication library.

Potential Mitigations

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 persistence layers such as Hibernate or Enterprise Java Beans, which can provide significant

protection against SQL injection if used properly.

Phase: Architecture and Design

Strategy: Parameterization

If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

Process SQL queries using prepared statements, parameterized queries, or stored procedures. These features should accept parameters or variables and support strong typing. Do not dynamically construct and execute query strings within these features using "exec" or similar functionality, since you may re-introduce the possibility of SQL injection.

Phase: Architecture and Design

Follow the principle of least privilege when creating user accounts to a SQL database. The database users should only have the minimum privileges necessary to use their account. If the requirements of the system indicate that a user can read and modify their own data, then limit their privileges so they cannot read/write others' data. Use the strictest permissions possible on all database objects, such as execute-only for stored procedures.

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.

Phase: Implementation

If you need to use dynamically-generated query strings in spite of the risk, use proper encoding and escaping of inputs. Instead of building your own implementation, such features may be available in the database or programming language. For example, the Oracle DBMS_ASSERT package can check or enforce that parameters have certain properties that make them less vulnerable to SQL injection. For MySQL, the mysql_real_escape_string() API function is available in both C and PHP.

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."

When constructing SQL query strings, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping.

Note that proper output encoding, escaping, and quoting is the most effective solution for preventing SQL injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent SQL injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, the name "O'Reilly" would likely pass the validation step, since it is a common last name in the English language. However, it cannot be directly inserted into the database because it contains the "'" apostrophe character, which would need to be escaped or otherwise handled. In this case, stripping the apostrophe might reduce the risk of SQL injection, but it would produce incorrect behavior because the wrong name would be recorded.

When feasible, it may be safest to disallow meta-characters entirely, instead of escaping them. This will provide some defense in depth. After the data is entered into the database, later processes may neglect to escape meta-characters before use, and you may not have control over those processes.

Phases: Testing; Implementation

Use automated static analysis tools that target this type of weakness. Many modern techniques use data flow analysis to minimize the number of false positives. This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Phase: Testing

Use 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.

Phase: Operation

Use an application firewall that can detect attacks against this weakness. This might not catch all attacks, and it might require some effort for customization. However, it can be beneficial in cases in which the code cannot be fixed (because it is controlled by a third party), as an emergency prevention measure while more comprehensive software assurance measures are applied, or to provide defense in depth.

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	77	Improper Sanitization of Special Elements used in a Command ('Command 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**
ChildOf	Category	751	2009 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	801	2010 Top 25 - Insecure Interaction Between Components	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	564	SQL Injection: Hibernate	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
MemberOf	View	635	Weaknesses Used by NVD	**Weaknesses Used by NVD (primary)635**
CanFollow	Weakness Base	456	Missing Initialization	Research Concepts1000

Relationship Notes

SQL injection can be resultant from special character mismanagement, MAID, or blacklist/whitelist problems. It can be primary to authentication errors.

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			SQL injection
7 Pernicious Kingdoms			SQL Injection
CLASP			SQL 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
WASC	19		SQL Injection

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
7	Blind SQL Injection	
66	SQL Injection	
108	Command Line Execution through SQL Injection	
109	Object Relational Mapping Injection	
110	SQL Injection through SOAP Parameter Tampering	

White Box Definitions

A weakness where the code path has:

1. start statement that accepts input and
2. end statement that performs an SQL command where

a. the input is part of the SQL command and

b. input contains SQL syntax (esp. query separator)

References

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 1: SQL Injection." Page 3. McGraw-Hill. 2010.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 12, "Database Input Issues" Page 397. 2nd Edition. Microsoft. 2002.

OWASP. "SQL Injection Prevention Cheat Sheet". <http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet>.

Steven Friedl. "SQL Injection Attacks by Example". 2007-10-10. <http://www.unixwiz.net/techtips/sql-injection.html>.

Ferruh Mavituna. "SQL Injection Cheat Sheet". 2007-03-15. <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>.

David Litchfield, Chris Anley, John Heasman and Bill Grindlay. "The Database Hacker's Handbook: Defending Database Servers". Wiley. 2005-07-14.

David Litchfield. "The Oracle Hacker's Handbook: Hacking and Defending Oracle". Wiley. 2007-01-30.

Microsoft. "SQL Injection". December 2008. <http://msdn.microsoft.com/en-us/library/ms161953.aspx>.

Microsoft Security Vulnerability Research & Defense. "SQL Injection Attack". <http://blogs.technet.com/swi/archive/2008/05/29/sql-injection-attack.aspx>.

Michael Howard. "Giving SQL Injection the Respect it Deserves". 2008-05-15. <http://blogs.msdn.com/sdl/archive/2008/05/15/giving-sql-injection-the-respect-it-deserves.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined
	7 Pernicious Kingdoms		Externally Mined
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci updated Time of Introduction	Cigital	External
2008-08-01	 added/updated white box definitions	KDM Analytics	External
2008-08-15	 Suggested OWASP Top Ten 2004 mapping	Veracode	External
2008-09-08	CWE Content Team updated Applicable Platforms, Common Consequences, Modes of Introduction, Name, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings	MITRE	Internal
2008-10-14	CWE Content Team updated Description	MITRE	Internal
2008-11-24	CWE Content Team updated Observed Examples	MITRE	Internal
2009-01-12	CWE Content Team updated Demonstrative Examples, Description, Enabling Factors for Exploitation, Modes of Introduction, Name, Observed Examples, Other Notes, Potential Mitigations, References, Relationships	MITRE	Internal
2009-03-10	CWE Content Team updated Potential Mitigations	MITRE	Internal
2009-05-27	CWE Content Team updated Demonstrative Examples, Name, Related Attack Patterns	MITRE	Internal
2009-07-17	KDM Analytics Improved the White Box Definition		External
2009-07-27	CWE Content Team updated Description, Name, White Box Definitions	MITRE	Internal
2009-12-28	CWE Content Team updated Potential Mitigations	MITRE	Internal
2010-02-16	CWE Content Team updated Demonstrative Examples, Detection Factors, Potential Mitigations, References, Relationships, Taxonomy Mappings	MITRE	Internal
2010-04-05	CWE Content Team updated Demonstrative Examples, Potential Mitigations	MITRE	Internal

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	SQL Injection
2008-09-09	Failure to Sanitize Data into SQL Queries (aka 'SQL Injection')
2009-01-12	Failure to Sanitize Data within SQL Queries (aka 'SQL Injection')
2009-05-27	Failure to Preserve SQL Query Structure (aka 'SQL Injection')
2009-07-27	Failure to Preserve SQL Query Structure ('SQL Injection')

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
JavaScript	5800567670153336	12/4/2015
VbScript	7089180910237385	8/3/2015
Objc	1302130541012371	8/3/2015