

VPN Clients Security Testing

iOS Client Validation Retest

NordVPN

Monday, March 15, 2021

VerSprite OffSec Team



Table of Contents

TABLE OF CONTENTS	2
VALIDATION RETEST MATRIX	3
(REMEDIATED) REALM DATABASE KEY STORED IN PLAINTEXT (CWE-312) – Low	4
(MITIGATED) LACK OF BINARY PROTECTIONS (CWE-693) – Low.....	5
(REMEDIATED) INSECURE STORAGE OF SENSITIVE INFORMATION IN MEMORY (CWE-693) – Low.....	6
(REMEDIATED) INFORMATION DISCLOSURE IN BINARY FILES (CWE-615) – Low	7

Validation Retest Matrix

Vulnerability	Status	Summary
<i>Realm Database Key Stored in Plaintext (CWE-312)</i>	Remediated	During the validation retest, VerSprite discovered that it is no longer possible to decrypt the contents of the encrypted Realm database using the hardcoded credentials previously found on the source code.
<i>Lack of Binary Protections (CWE-693)</i>	Mitigated	We found that it is still possible to run the NordVPN client on a jailbroken iOS device. However, an warning is provided to the users alerting of the risks of running the application on jailbroken devices.
<i>Insecure Storage of Sensitive Information in Memory (CWE-693)</i>	Remediated	We found that it is no longer possible to obtain sensitive information such as the user password from the process memory dump.
<i>Information Disclosure in Binary Files (CWE-615)</i>	Remediated	VerSprite found that it is no longer possible to obtain the usernames of NordVPN employees by analyzing the iOS application binary strings.

Figure 1 – Validation Retest Matrix

(Remediated) Realm Database Key Stored in Plaintext (CWE-312) – Low

Validation Retest Notes

During the validation retest, VerSprite discovered that it is no longer possible to decrypt the Realm database with the hardcoded credentials previously found on the source code. A new database called default.encrypted_v2.realm has been created which is encrypted with an unknown passphrase.

As can be observed as follows, it was not possible to decrypt the file with the passphrase used previously:

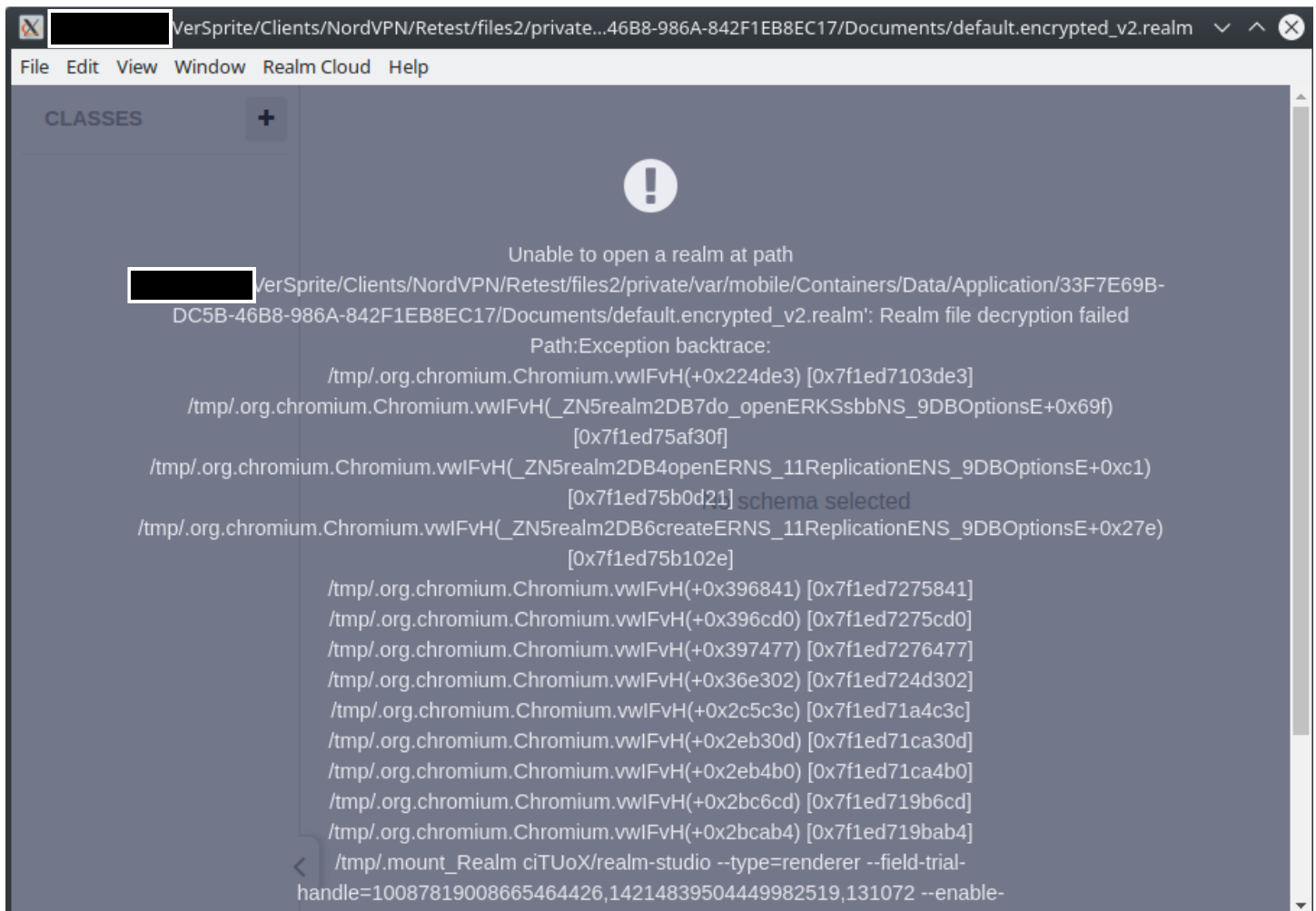


Figure 2 - Realm database with hardcoded password

(Mitigated) Lack of Binary Protections (CWE-693) – Low

Validation Retest Notes

During the validation retest, we found that it is still possible to run the NordVPN client on a jailbroken iOS device. In the following proof of concept, we logged into the jailbroken device with root credentials. Next, we show that the NordVPN client was running and proceeded to list the application files

```

root@192.168.0.10:~$ ssh root@192.168.0.10
root@192.168.0.10's password:
VSs-iPad:~ root# ps aux | grep -i Nord
mobile      2806    1.5 12.9  5312880 263664  ??  Ss   Wed09PM   0:42.72 /var/containers/Bundle/Application/1E76E005-5C34-4A18-8943-047BC33910A5/NordVPN.app/NordVPN
root        3005    0.0  0.2  4213104  4560 s000  R+   11:23AM   0:00.01 grep -i Nord
VSs-iPad:~ root#
  
```

Figure 3 - NordVPN application

```

VSs-iPad:/private/var/mobile/Containers/Data/Application/4D3D2F08-32C9-4BEA-A738-BDBC7F5C4B1 root# cd /var/containers/Bundle/Application/1E76E005-5C34-4A18-8943-047BC33910A5/NordVPN.app root# ls -al
total 28468
drwxr-xr-x 119  _installd  _installd    3808 Feb 18 06:11 ./
drwxr-xr-x  6  _installd  _installd    192 Mar 11 21:36 ../
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ActionIndicationCell.nib/
-rw-r--r--  1  _installd  _installd  134436 Dec 30 10:30 Aller_Rg.ttf
-rw-r--r--  1  _installd  _installd   1197 Dec 30 10:30 AppContextNotificationView.nib
-rw-r--r--  1  _installd  _installd   5336 Dec 30 10:30 AppIcon60x60@2x.png
-rw-r--r--  1  _installd  _installd   7305 Dec 30 10:30 AppIcon76x76@2x-ipad.png
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 AppearanceViewController.nib/
-rw-r--r--  1  _installd  _installd 10502696 Dec 30 10:31 Assets.car
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 AutoConnectViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 BackButtonView.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 BadgeView.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CardDetailCell.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CardSectionHeaderView.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CityListCardViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CloseButtonView.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ConnectionCardViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ConnectionHelpCell.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ConnectionIssuesViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ConnectionRatingView.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ConnectionStatusBarIpadView.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ConnectionStatusBarView.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 ContactViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CountriesListViewController.nib/
drwxr-xr-x  5  _installd  _installd    160 Feb 18 06:10 CrossDeviceCollectionCell.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CrossDeviceUsageViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CurrentAppContextViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CustomDNSCell.nib/
-rw-r--r--  1  _installd  _installd   3218 Dec 30 10:31 CustomPageBodyTextCell.nib
-rw-r--r--  1  _installd  _installd   4493 Dec 30 10:31 CustomPageBulletAndTextCell.nib
-rw-r--r--  1  _installd  _installd   2849 Dec 30 10:31 CustomPageHeaderImageCell.nib
-rw-r--r--  1  _installd  _installd   3250 Dec 30 10:31 CustomPageHeadlineCell.nib
-rw-r--r--  1  _installd  _installd   4870 Dec 30 10:31 CustomPageIconAndTextCell.nib
-rw-r--r--  1  _installd  _installd   5692 Dec 30 10:31 CustomPagePlanSelectCell.nib
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CustomPageTimerCell.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 CustomPageViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 DebugViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 DeepLinkConnectViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 DeepLinkSnoozeViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 DetectedLeaksViewController.nib/
drwxr-xr-x  4  _installd  _installd    128 Feb 18 06:10 EmptyFavoritesView.nib/
  
```

Figure 4 - Application files

However, we found that an alert message information the user of the risks involved in running the application in a jailbroken device is presented when the application is first launched.

(Remediated) Insecure Storage of Sensitive Information in Memory (CWE-693) – Low

Validation Retest Notes

During the validation retest we found that it is still possible to obtain the username from the NordVPN process memory as can be observed in the following screenshot.

```
~/bin/fridump3$ python3 fridump3.py -s -u "NordVPN"

fridump3

Current Directory: ~/bin/fridump3
Output directory is set to: ~/bin/fridump3/dump
Creating directory...
Starting Memory dump...
Oops, memory access violation!#####-----] 65.02% Complete
Oops, memory access violation!#####-----] 81.42% Complete
Oops, memory access violation!#####-----] 86.07% Complete
Oops, memory access violation!#####-----] 86.69% Complete
Oops, memory access violation!#####-----] 87.0% Complete
Oops, memory access violation!#####-----] 87.31% Complete
Oops, memory access violation!#####-----] 88.54% Complete
Oops, memory access violation!#####-----] 89.16% Complete
Oops, memory access violation!#####-----] 89.47% Complete
Oops, memory access violation!#####-----] 90.09% Complete
Oops, memory access violation!#####-----] 91.02% Complete
Running strings on all files:#####-----] 98.14% Complete
Progress: [#####] 100.0% Complete

Finished!
```

Figure 5 - Memory dump

```
~/bin/fridump3/dump$ cat strings.txt | grep -i pentest
pentest1
pentest1
```

Figure 6 – Username

However, no sensitive information such as the user password could be found in the process dump.

(Remediated) Information Disclosure in Binary Files (CWE-615) – Low

Validation Retest Notes

During the validation retest, VerSprite found that it is no longer possible to obtain the usernames of NordVPN employees by analyzing the iOS application binary strings:

```
~/VerSprite/Clients/NordVPN/Retest/files2/var/containers/Bundle/Application/BB2A196F-E55D-411A-B42D-4D725F5871BC/NordVPN.app$ strings NordVPN | grep -i Users
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Screens/RootViewController/RootViewController.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Views/RecentServersCell.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Screens/MessageViewController/MessageViewController.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Views/CardCanvasView.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Screens/CrossDeviceUsageViewController/CrossDeviceUsageViewController.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Views/AppContextNotificationView.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Screens/CurrentAppContextViewController/CurrentAppContextViewController.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Screens/CurrentAppContextViewController/States/LoginContextState.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Views/NordHUDView.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Views/RateCell.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Extensions/UITableView.swift
_TtC7NordVPNI/UserSessionHelper
userSession
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Screens/CardCoordinator/CardCoordinator.swift
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/NordVPN/Views/NordHUD.swift
/Users/maximshoustin/AppsFlyer/projects/BUILD_MACHINE/build-machine-sdk/workspace/ios_sdk_framework_test/AppsFlyerLib/AppsFlyerLib/AppsFlyerHTTPClient.m
Failed to remove all users writes on disk!
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/Pods/FirebaseDatabase/FirebaseDatabase/Sources/Persistence/FLevelDBStorageEngine.m
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/Pods/FirebaseDatabase/FirebaseDatabase/Sources/Core/FPersistentConnection.m
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/Pods/FirebaseDatabase/FirebaseDatabase/Sources/Core/FRepo.m
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/Pods/FirebaseDatabase/FirebaseDatabase/Sources/Snapshot/FSnapshotUtilities.m
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/Pods/FirebaseDatabase/FirebaseDatabase/Sources/third_party/SocketRocket/FSRWebSocket.m
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/Pods/FirebaseDatabase/FirebaseDatabase/Sources/Realtime/FWebSocketConnection.m
/Users/runner/work/firebase-ios-sdk/firebase-ios-sdk/FirebasePerformance/Sources/Gauges/CPU/FPRCPUGaugeCollector.m
/Users/builds/9d19d54f/0/nordvpn-ios-app/nordvpn-ios-app/Pods/FirebaseRemoteConfig/FirebaseRemoteConfig/Sources/RCNConfigDBManager.m
UserSessionHelper
userSession
```

Figure 7 - Binary contents