VPN Clients Security Testing
Android Client Validation Retest

NordVPN

Tuesday, April 6, 2021

VerSprite OffSec Team

Table of Contents

TABLE OF CONTENTS **2**

VALIDATION RETEST MATRIX **3**

(REMEDIATED) CLEARTEXT STORAGE OF SENSITIVE INFORMATION (CWE-312) – LOW 4
(REMEDIATED) REALM DATABASE KEY STORED IN PLAINTEXT (CWE-312) – LOW 5
(RISK ACCEPTED) APK V1 SIGNATURE SUPPORTED (CWE-327) – LOW 6
(RISK ACCEPTED) LACK OF BINARY PROTECTIONS (CWE-693) – LOW 7
(MITIGATED) LACK OF MEMORY PROTECTIONS (CWE-693) – LOW 8

Validation Retest Matrix

Vulnerability	Status	Summary
Cleartext Storage of Sensitive Information (CWE-312)	*Remediated*	The application is now storing sensitive information in an encrypted manner.
Realm Database Key Stored in Plaintext (CWE-312)	*Remediated*	The application is now using sqlite3 databases instead of Realm databases.
APK v1 Signature Supported (CWE-327)	*Risk Accepted*	The application is still signed with the v1 signature scheme. A business decision was made to support Android versions below 7, so APK v1 signature won't be removed.
Lack of Binary Protections (CWE-693)	*Risk Accepted*	It is still possible to run the NordVPN application in rooted Android devices. No warning message of any kind is displayed to the user. A business decision was made to allow the NordVPN application to run on rooted devices without any limitations, so this information is only stored in logs at the moment.
Lack of Memory Protections (CWE-693)	*Mitigated*	Several shared libraries for the NordVPN application still lack several protection mechanisms. However, some libraries are not compiled by NordVPN. Also, for other libraries additional information is required at compile time in order to be fortified, which is not always known. As the maximum protection viable was added to the libraries, this issue is marked as "Mitigated".

Figure 1 – Validation Retest Matrix

(Remediated) Cleartext Storage of Sensitive Information (CWE-312) – Low

Validation Retest Notes

During the validation retest, we found the application is still storing sensitive information in the device, but encrypting it first. For example, in the previous version, the MQTT credentials were stored unencrypted inside a Realm database (*com.nordvpn.android.tokens*). In the new version, they are stored encrypted inside a sqlite3 database (*Settings.db*), as can be seen in the following output:

```
root@vbox86p:/data/data/com.nordvpn.android/databases # sqlite3 Settings.db
SQLite version 3.8.10.2 2015-05-20 18:17:19
Enter ".help" for usage hints.
sqlite> .tables
AppMessageContentDataEntity             MQTTCredentialsEntity
AppMessageContentEntity                 NCMessageDataEntity
AppMessageDealDataEntity                PreferredTechnologyEntity
AppMessageEntity                        ProcessablePurchaseEntity
AppMessageSubscriptionStatusDataEntity  RatingNotificationDataEntity
AutoConnectEntity                       RecentSearchEntity
BreachReportEntity                      TrustedAppEntity
BreachSettingEntity                     android_metadata
ConnectionHistoryEntity                 room_master_table
DnsConfigurationEntity
sqlite> select * from MQTTCredentialsEntity;
0|mcy9Bd4ii7X1tTGuMbwgpDuBdv0YpINnlR3+r6q7c+TE7lS5seCEKCDb9IEPp44ymEVik8OLtRfJ
ht1tlSIAKtE=
|mcy9Bd4ii7X1tTGufb5k5jfMbvYesMFrxFr54KWuN6HStVqqtK7EcT+K+NVTrNRvmxo08//zEmkd
JyGyDPL06D7NR1hPx+dDuhQbOKdb7hygsw0S79xxH4LVe48HFyUY/n06xhI2CJP5tpM2jdcX8NdG
WVeq008w0SRdg88MZJ267iWbhpGnoV/STKvcLdmjVGlGJd047hfVcN9x
|mcy9Bd4ii7X1tTGucqUilFGdb9cY2J47yFmZu7S8UKGv53CKmKO6fmfs04qOX4eHeqTXzuupy9aC
l5c8
|1615827996051
```

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

Validation Retest Notes

During the validation retest, we found that the NordVPN application is not using Realm databases anymore, and switched to sqlite3 databases instead, as can be seen from the following output:

```
root@vbox86p:/data/data/com.nordvpn.android/databases # ls
Main.db
Main.db-shm
Main.db-wal
Moose.db
Settings.db
Settings.db-shm
Settings.db-wal
com.google.android.datatransport.events
com.google.android.datatransport.events-journal
google_analytics_v4.db
google_analytics_v4.db-journal
google_app_measurement_local.db
google_app_measurement_local.db-journal
root@vbox86p:/data/data/com.nordvpn.android/databases #
```

(Risk Accepted) APK v1 Signature Supported (CWE-327) – Low

Validation Retest Notes

During the validation retest we found that the application is still signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0 as shown in the following excerpt:

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=PA, ST=Panama, L=Panama, O=Tefincom, OU=Mobile Development, CN=Alex Weblowsky
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-01-22 07:19:25+00:00
Valid To: 2041-01-15 07:19:25+00:00
Issuer: C=PA, ST=Panama, L=Panama, O=Tefincom, OU=Mobile Development, CN=Alex Weblowsky
Serial Number: 0x724d9712
Hash Algorithm: sha256
md5: ae8e3397a9180b209684ede51d74f901
sha1: faba42561be52057f670b4412fd513ef687ca47a
sha256: bc64ae0725af656b3b10b684cd1df4c9d6b7f81bc5dc32df3a3b2ce94ce61466
sha512:
059e35c38725cb7ebfda0d479aeec73bf300d42c52b9046756f87b2fdd877df8bf6dfb39c9abf0a19f2decd166190bdd3bbb7948f60b4
5d8f39d59f0b70eb4c2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 542aea74b643c3d5b7ddb60e04e356983eaf5f1b7c3a7dddb16e2483da1f83a9
```

(Risk Accepted) 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 application on a rooted Android device. It can be seen in the following screenshot a Terminal Emulator with a root shell running simultaneously with the NordVPN application:

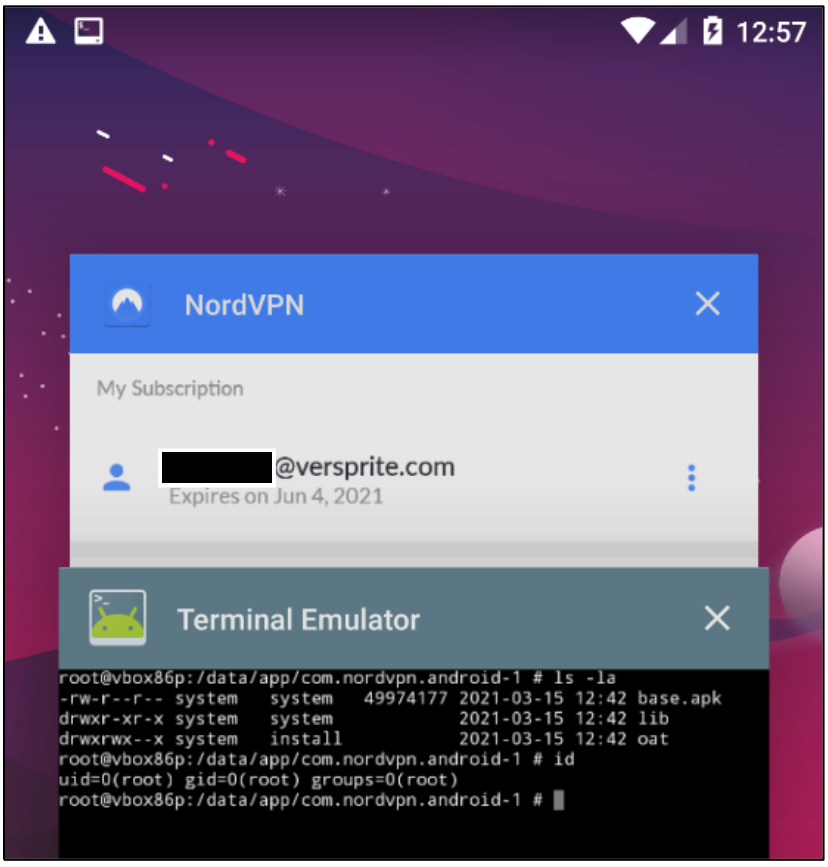

Figure 2 - NordVPN application and Terminal Emulator with a root shell running simultaneously.

No warning message is ever displayed to the user at startup nor while using the application.

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

Validation Retest Notes

During the validation retest, we found several shared libraries still lacking protection mechanisms. In the following table we detail the shared libraries found in the new version and whether the protection mechanism is enabled (or not):

Name	NX	Stack Canary	RELRO	FORTIFY
lib/x86_64/libcrashlytics-common.so	True	True	False	True
lib/x86_64/libcrashlytics-handler.so	True	True	False	True
lib/x86_64/libcrashlytics.so	True	True	False	True
lib/x86_64/libnudler.so	True	True	True	True
lib/x86_64/libcrashlytics-trampoline.so	True	False	False	False
lib/x86_64/libmooseworker.so	True	True	True	True
lib/x86_64/libmoosenordvpnapp.so	True	True	True	True
lib/x86_64/libopenvpn.so	True	True	True	True
lib/x86_64/libnordlynx.so	True	True	True	True
lib/x86_64/libmoosenordvpnappjava.so	True	True	True	False
lib/x86_64/libmooseworkerjava.so	True	True	True	False
lib/x86_64/libovpnexec.so	True	True	True	False
lib/arm64-v8a/libcrashlyticscommon.so	True	True	False	True
lib/arm64-v8a/libcrashlytics-handler.so	True	True	False	True
lib/arm64-v8a/libcrashlytics.so	True	True	False	True
lib/arm64-v8a/libnudler.so	True	True	True	True
lib/arm64-v8a/libcrashlyticstrampoline.so	True	False	False	False
lib/arm64-v8a/libmooseworker.so	True	True	True	True
lib/arm64-v8a/libmoosenordvpnapp.so	True	True	True	True
lib/arm64-v8a/libopenvpn.so	True	True	True	True
lib/arm64-v8a/libnordlynx.so	True	True	True	True
lib/arm64-v8a/libmoosenordvpnappjava.so	True	True	True	False
lib/arm64-v8a/libmooseworkerjava.so	True	True	True	False
lib/arm64-v8a/libovpnexec.so	True	True	True	False
lib/x86/libcrashlytics-common.so	True	True	False	False
lib/x86/libcrashlytics-handler.so	True	True	False	False
lib/x86/libcrashlytics.so	True	True	False	False
lib/x86/libnudler.so	True	True	True	False
lib/x86/libcrashlytics-trampoline.so	True	True	False	False
lib/x86/libmooseworker.so	True	True	True	False
lib/x86/libmoosenordvpnapp.so	True	True	True	False
lib/x86/libopenvpn.so	True	True	True	True
lib/x86/libnordlynx.so	True	True	True	True
lib/x86/libmoosenordvpnappjava.so	True	True	True	False
lib/x86/libmooseworkerjava.so	True	True	True	False
lib/x86/libovpnexec.so	True	True	True	False
lib/armeabi-v7a/libcrashlyticscommon.so	True	True	False	False
lib/armeabi-v7a/libcrashlyticshandler.so	True	True	False	False

lib/armeabi-v7a/libcrashlytics.so	True	True	False	False
lib/armeabi-v7a/libnudler.so	True	True	True	False
lib/armeabi-v7a/libcrashlyticstrampoline.so	True	False	False	False
lib/armeabi-v7a/libmooseworker.so	True	True	True	False
lib/armeabiv7a/libmoosenordvpnapp.so	True	True	True	False
lib/armeabi-v7a/libopenvpn.so	True	True	True	True
lib/armeabi-v7a/libnordlynx.so	True	True	True	True
lib/armeabiv7a/libmoosenordvpnappjava.so	True	True	True	False
lib/armeabiv7a/libmooseworkerjava.so	True	True	True	False
lib/armeabi-v7a/libovpnexec.so	True	True	True	False