MOBSF

ANDROID STATIC ANALYSIS REPORT

SuperVPN (2.6.4)

File Name:	supervpn-free-vpn-client_2.6.4.apk
Package Name:	com.jrzheng.supervpnfree
Average CVSS Score:	5.9
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	5/285

FILE INFORMATION

File Name: supervpn-free-vpn-client_2.6.4.apk
Size: 10.58MB
MD5: e537bfecc6ff3a870c654a751e9b03b7
SHA1: b572695f1d2f7ac1f0e52f6c749691ffccc7963c
SHA256: f05bf86039d9dd968f7cad80ff693027792ed1d8405682a35e165e7fdb9c490f

APP INFORMATION

App Name: SuperVPN
Package Name: com.jrzheng.supervpnfree
Main Activity: com.supersoft.supervpnfree.activity.MainActivity
Target SDK: 28
Min SDK: 16
Max SDK:
Android Version Name: 2.6.4
Android Version Code: 94

APP COMPONENTS

Activities: 16
Services: 8
Receivers: 3
Providers: 4
Exported Activities: 0
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: CN=ron zheng
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-08-09 04:41:30+00:00
Valid To: 2037-08-03 04:41:30+00:00
Issuer: CN=ron zheng
Serial Number: 0x50233f7a
Hash Algorithm: sha1
md5: fbc2618fc6554688da1b52f4fdf3907f
sha1: 03cc844c25111f108a1e2336df9cdf5864e9a3fb
sha256: 5200d5e89b55d901033896db249503efb28479279158101a6a0d3bea4c7ab906
sha512:
953e8f4ad873168f98d4bb59fc4e56cec1abe52c0b07c44cd7ac4a5668bfe1dc5c0abe1e1b04a548c2ebcddd1f22c469e96b3013e7c4255594a29e0ba7cd9b9e

Certificate Status: Bad
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use
com.android.vending.BILLING	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial

			number of this phone, whether a call is active, the number that call is connected to and so on.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

APKID ANALYSIS

FILE	DETAILS
assets/audience_network.dex	FINDINGS: Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check ro.kernel.qemu check FINDINGS: Compiler — dexlib 1.x
classes.dex	FINDINGS: Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check FINDINGS: Anti Debug Code — Debug.isDebuggerConnected() check FINDINGS: Compiler — dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
		The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level

Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
Application Data can be Backed up [android:allowBackup] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
TaskAffinity is set for Activity (com.supersoft.supervpnfree.activity.VpnDialogActivity)	high	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
Launch Mode of Activity (com.supersoft.supervpnfree.activity.VpnDialogActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	c/c/b/c/j/i.java c/c/b/c/j/h.java c/c/a/c.java c/b/a/r/g.java c/b/a/t/j.java c/b/a/t/b.java c/b/a/t/h.java c/b/a/s/b.java b/p/k0.java b/p/s.java b/p/j0.java b/j/a/d.java b/g/k/c0.java b/g/k/d0/c.java b/g/k/d0/d.java b/e/f.java b/e/g.java b/e/b.java b/b/a/b/b.java com/bumptech/glide/load/i.java com/bumptech/glide/load/h.java com/bumptech/glide/load/n/c.java com/bumptech/glide/load/n/m.java com/bumptech/glide/load/n/w.java com/bumptech/glide/load/n/z/c.java com/bumptech/glide/load/n/z/j.java com/bumptech/glide/load/n/z/n.java com/bumptech/glide/load/o/j.java com/bumptech/glide/load/o/g.java com/bumptech/glide/load/o/m.java com/bumptech/glide/load/p/c/o.java com/bumptech/glide/load/p/c/g.java com/bumptech/glide/load/p/c/m.java com/bumptech/glide/load/p/c/h.java com/bumptech/glide/load/p/g/f.java d/a/a/a/c.java d/a/a/a/n/b/b.java
			c/c/b/c/j/h.java c/c/b/c/k/a.java c/b/a/c.java

The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	c/b/a/n/d.java c/b/a/n/e.java c/b/a/o/f.java c/b/a/o/l.java c/b/a/o/o.java c/b/a/o/e.java c/b/a/o/k.java c/b/a/o/n.java c/b/a/p/e.java c/b/a/r/g.java c/b/a/r/i/i.java c/b/a/t/k/a.java c/a/b/b/a.java c/a/a/a/a.java b/n/c.java b/n/a.java b/p/f0.java b/p/g0.java b/p/z.java b/p/d0.java b/p/e0.java b/p/y.java b/m/b/c.java b/m/a/b.java b/j/a/e.java b/j/a/j.java b/j/a/a.java b/j/a/n.java b/j/a/b.java b/l/a/a.java b/g/j/b.java b/g/d/i.java b/g/d/f.java b/g/d/d.java b/g/d/e.java b/g/d/b.java b/g/d/h.java b/g/k/e.java b/g/k/g.java b/g/k/u.java b/g/k/x.java b/g/k/b.java b/g/k/v.java b/g/k/d0/d.java b/q/a/a/i.java b/a/m/g.java b/a/k/a/a.java b/i/b/a.java com/bumptech/glide/load/n/j.java com/bumptech/glide/load/n/g.java com/bumptech/glide/load/n/p.java com/bumptech/glide/load/n/h.java com/bumptech/glide/load/n/y.java com/bumptech/glide/load/n/b0/a.java com/bumptech/glide/load/n/z/j.java com/bumptech/glide/load/n/z/k.java com/bumptech/glide/load/n/a0/i.java com/bumptech/glide/load/n/a0/e.java com/bumptech/glide/load/o/f.java com/bumptech/glide/load/o/c.java com/bumptech/glide/load/o/d.java com/bumptech/glide/load/o/s.java com/bumptech/glide/load/o/t.java com/bumptech/glide/load/p/c/i.java com/bumptech/glide/load/p/c/l.java

			com/bumptech/glide/load/p/c/c.java com/bumptech/glide/load/p/c/k.java com/bumptech/glide/load/p/c/u.java com/bumptech/glide/load/p/c/p.java com/bumptech/glide/load/p/c/w.java com/bumptech/glide/load/p/g/d.java com/bumptech/glide/load/p/g/j.java com/bumptech/glide/load/p/g/a.java com/bumptech/glide/load/m/l.java com/bumptech/glide/load/m/j.java com/bumptech/glide/load/m/b.java com/bumptech/glide/load/m/o/c.java com/bumptech/glide/load/m/o/e.java com/makeramen/roundedimageview/b.java com/makeramen/roundedimageview/RoundedImageView.java com/supersoft/supervpnfree/activity/f/a.java com/supersoft/supervpnfree/logic/TrustedCertificateManager.java com/supersoft/supervpnfree/logic/CharonVpnService.java d/a/a/a/b.java d/a/a/a/n/c/a.java d/a/a/a/n/b/x.java
IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor OWASP MASVS: MSTG-CODE-2	c/d/a/c/d.java d/a/a/a/c.java d/a/a/a/m.java
MD5 is a weak hash known to have hash collisions.	high	CVSS V2: 7.4 (high) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	c/d/a/d/e.java okio/Buffer.java
The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 (high) CWE: CWE-330 - Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	c/d/a/a/c.java
App creates temp file. Sensitive information should never be written into a temp file.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	b/n/c.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 (high) CWE: CWE-312 - Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/h.java com/bumptech/glide/load/n/c.java com/bumptech/glide/load/n/o.java com/bumptech/glide/load/n/w.java com/supersoft/supervpnfree/logic/VpnStateService.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/supersoft/supervpnfree/activity/a.java d/a/a/a/d.java
This App may have root		CVSS V2: 0 (info)	

detection capabilities.	secure	**OWASP MASVS:** MSTG-RESILIENCE-1	d/a/a/a/n/b/i.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
e.crashlytics.com	good	**IP:** 54.243.38.81 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
bit.ly	good	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
github.com	good	**IP:** 140.82.118.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
supervpn-bda69.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.unblockv.fun	good	**IP:** 104.27.145.45 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
api.novatech.fun	good	**IP:** 104.28.19.97 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
		IP: 96.126.99.114 **Country:** United States of America **Region:** California

www.supervpn.cc	good	**City:** Fremont **Latitude:** 37.548271 **Longitude:** -121.988571 **View:** Google Map
api.novatech.site	good	**IP:** 104.31.90.55 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
settings.crashlytics.com	good	**IP:** 216.58.206.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.gecko.fun	good	**IP:** 104.27.153.116 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
play.google.com	good	**IP:** 172.217.169.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://api.gecko.fun https://api.novatech.fun https://api.novatech.site https://api.unblockv.fun	c/d/a/c/d.java
data:image	com/bumptech/glide/load/o/e.java
http://www.supervpn.cc/background.html https://play.google.com/store/apps/details?id=	com/supersoft/supervpnfree/activity/MainActivity.java
https://e.crashlytics.com/spi/v2/events	d/a/a/a/n/g/l.java
https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings	d/a/a/a/n/g/r.java
https://supervpn-bda69.firebaseio.com	

https://github.com/vinc3m1 https://github.com/vinc3m1/RoundedImageView https://github.com/vinc3m1/RoundedImageView.git http://bit.ly/superforfree	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://supervpn-bda69.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	URL
Facebook Ads	https://reports.exodus-privacy.eu.org/trackers/65
Google Ads	https://reports.exodus-privacy.eu.org/trackers/71
Google CrashLytics	https://reports.exodus-privacy.eu.org/trackers/27
Google DoubleClick	https://reports.exodus-privacy.eu.org/trackers/5
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.