MOBSF

ANDROID STATIC ANALYSIS REPORT

VA Video Connect (1.10.1)

File Name:	gov.va.vamf.vavideoconnect_58.apk
Package Name:	gov.va.vamf.vavideoconnect
Scan Date:	Sept. 1, 2025, 1:26 p.m.
App Security Score:	59/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	1	2	1

FILE INFORMATION

File Name: gov.va.vamf.vavideoconnect_58.apk
Size: 48.69MB
MD5: 564dc9484c8fa5c4483a07c6420a5580
SHA1: e8bc6867008b9987f6a0d0b2e1917444723dcf90
SHA256: df6a2e7a4c919b07e997e1fa37a61796f1ba8017024c41a9320fb9307b437de5

APP INFORMATION

App Name: VA Video Connect
Package Name: gov.va.vamf.vavideoconnect
Main Activity: gov.va.vamf.vavideoconnect.ui.launch.LaunchScreen
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 1.10.1

Android Version Code: 58

APP COMPONENTS

Activities: 8
Services: 12
Receivers: 5
Providers: 3
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-07 15:03:52+00:00
Valid To: 2051-07-07 15:03:52+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x20a1afeb2bfcdd020d7559cfef22ae4e6fa7b554
Hash Algorithm: sha256
md5: b52ab2f9da6111dc3c8b151e7efc7e73
sha1: 327f03e72a35762e0a25ee3854f30b181ffbef6c
sha256: 5db31b93848a25e41f696387d672e4a0b130c93fecff56bc43739f9a1d49ab8d
sha512: b1e4877ff92e5f9a608e99ba7222a8cae36439676560cc005fa75551f3f28cfb967dd52c7246c32f10df7d0128ee7ed2a9177dec6a4fba351e1a6fc4d0194cf3
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 33de335d3b1cc48cd8ce50b3e29a7d305dce113a3110e7e2ca594b330c86590c
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.FOREGROUND_SERVICE_CAMERA	normal	allows foreground services with camera use.	Allows a regular application to use Service.startForeground with the type "camera".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
gov.va.vamf.vavideoconnect.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to nearby Bluetooth devices.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

APKID ANALYSIS

FILE	DETAILS
564dc9484c8fa5c4483a07c6420a5580.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check possible VM check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
gov.va.vamf.vavideoconnect.ui.launch.LaunchScreen	Schemes: https://, Hosts: care.va.gov, care1.va.gov, care2.va.gov, dev.care2.va.gov, vvs.mapsandbox.net, pexip.mapsandbox.net, veteran.apps.va.gov, veteran.mobilehealth.va.gov, veteran.mobile.va.gov, Path Patterns: /vvc-app/.*, /go/.*,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App Link assetlinks.json file not found [android:name=gov.va.vamf.vavideoconnect.ui.launch.LaunchScreen] [android:host=https://veteran.apps.va.gov]	high	App Link asset verification URL (https://veteran.apps.va.gov/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
2	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	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

HIGH: **0** | WARNING: **4** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ekodevices/ekoconnect/utils/AndroidECLogger.java com/ekodevices/ekoconnect/utils/ConsoleECLogger.java com/ekodevices/library/EDAssetTransferManager$sendNextWindow$1$1.java com/ekodevices/library/EDAssetTransferManager.java com/ekodevices/library/EDAuscultationManagerWrapper.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a com/ekodevices/library/EDLibCore.java com/ekodevices/library/adpcm/EkoDuoAudioStreamer$streamAudioToDevice$1.java com/ekodevices/library/device/EDCore2Device.java com/ekodevices/library/device/EDCoreDevice.java com/ekodevices/library/device/EDDevice$Companion$decompressAsync$1.java com/ekodevices/library/device/EDDevice$startBulkAssetTransferSendAsync$1.java com/ekodevices/library/device/EDDevice.java com/ekodevices/library/device/EDDuo2Device.java com/ekodevices/library/device/EDDuo3Device.java com/ekodevices/library/device/EDDuoDevice.java com/ekodevices/library/ota/CustomFileReader_v0.java com/ekodevices/library/ota/Duo15OTAHandler.java com/ekodevices/library/ota/EDOTAManager$startJobs$1.java com/ekodevices/library/ota/EDOTAManager$startJobs$2.java com/ekodevices/library/ota/EDOTAManager.java com/ekodevices/library/ota/OTAFirmwareWrite_v0.java com/ekodevices/library/ota/OTAFirmwareWrite_v1.java com/ekodevices/library/ota/OTAResponseReceiver_v0.java com/ekodevices/library/ota/OTAResponseReceiver_v1.java com/ekodevices/library/utils/EDBGAutoRecordManager.java com/ekodevices/library/utils/EDCEAutoRecordManager$startRecording$2$1.java com/ekodevices/library/utils/EDCEAutoRecordManager.java com/ekodevices/library/utils/SignalQualityAlgorithmManager.java com/ekodevices/library/utils/ZipDecompressor.java com/ekodevices/ui/graph/EkoGraphView.java com/ekodevices/ui/graph/EkoTimer.java com/ekodevices/ui/graph/config/EkoGraphConfiguration.java com/ekodevices/ui/graph/gl/AbstractGLView.java com/ekodevices/ui/graph/gl/GLESUtils.java com/ekodevices/ui/graph/gl/GLGraphView$onSurfaceChanged$2.java com/ekodevices/ui/graph/gl/GLGraphView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ekodevices/ui/graph/gl/MultiSampleConfigChooser.java com/ekodevices/ui/graph/util/AndroidEkoLogger.java
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/ekodevices/ui/graph/util/ConsoleEkoLogger.java com/twilio/audioswitch/android/ProductionLogger.java dagger/android/AndroidInjection.java gov/va/mobile/vamf/pulse/client/log/SystemPulseLogger.java gov/va/vamf/vavideoconnect/pulse/PulseDelegate.java gov/va/vamf/vavideoconnect/pulse/VVCPulseLogger.java gov/va/vamf/vavideoconnect/services/api/vsis/ParticipantChangeListener$requestParticipantAddress$1.java gov/va/vamf/vavideoconnect/services/api/vsis/ParticipantChangeListener.java gov/va/vamf/vavideoconnect/services/config/ConfigService.java gov/va/vamf/vavideoconnect/services/videoconference/CallService.java gov/va/vamf/vavideoconnect/services/videoconference/ClearCallService.java gov/va/vamf/vavideoconnect/services/videoconference/PeerConnectionStatsKt.java gov/va/vamf/vavideoconnect/services/videoconference/PexipApi.java gov/va/vamf/vavideoconnect/ui/bluetoothconnect/BluetoothManager$scanObserver$1$1$1.java gov/va/vamf/vavideoconnect/ui/bluetoothconnect/BluetoothManager.java gov/va/vamf/vavideoconnect/ui/bluetoothconnect/device/BloodPressure.java gov/va/vamf/vavideoconnect/ui/bluetoothconnect/device/Peripheral.java gov/va/vamf/vavideoconnect/ui/bluetoothconnect/device/PulseOximeter.java gov/va/vamf/vavideoconnect/ui/bluetoothconnect/device/Scale.java gov/va/vamf/vavideoconnect/ui/bluetoothconnect/device/Thermometer.java gov/va/vamf/vavideoconnect/ui/e911/E911FormDialogFragment$openDialog$2$1.java gov/va/vamf/vavideoconnect/ui/e911/E911FormDialogFrag

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ment.java gov/va/vamf/vavideoconnect/ui/e911/E911FormViewModel$preValidateAddress$1.java gov/va/vamf/vavideoconnect/ui/e911/E911FormViewModel$requestAllAddresses$1.java gov/va/vamf/vavideoconnect/ui/e911/E911FormViewModel$requestEmergencyContact$1.java gov/va/vamf/vavideoconnect/ui/e911/E911FormViewModel$requestParticipantAddress$1.java gov/va/vamf/vavideoconnect/ui/e911/E911FormViewModel$saveParticipantAddress$1.java gov/va/vamf/vavideoconnect/ui/e911/E911SaveAddressDialogFragment.java gov/va/vamf/vavideoconnect/ui/inviteparticipant/InviteParticipantViewModel$inviteParticipant$1.java gov/va/vamf/vavideoconnect/ui/launch/LaunchActivityViewModel$retrieveAppointmentVMRStatus$1$1$1.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivity$bindClearCallService$1.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivity.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivityViewModel$deletePatientInfo$2.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivityViewModel$pullSilentSignals$1.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivityViewModel$retrievePatientInfo$address$1.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivityViewModel$savePatientInfo$1.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivityViewModel$saveVeteran$1.java gov/va/vamf/vavideoconnect/ui/videoconference/ConferenceActivityViewModel.java gov/va/vamf/vavideoconnect/utils/SingleLiveEvent.java gov/va/vamf/vavideoconnect/vision/BitmapUtils.java gov/va/vamf/vavideoconnect/vision/SegmentationProcessor.java gov/va/vamf/vavideoconnect/vision/VisionProcessorBase.java org/webrtc/VVCCamera1Session.java timber/log/Timber.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/ekodevices/ekoconnect/EkoConnect.java com/ekodevices/ekoconnect/auth/ECAuthCredentials.java com/ekodevices/ekoconnect/auth/ECAuthHeaders.java com/ekodevices/library/ota/Duo15OTAHandler.java gov/va/vamf/vavideoconnect/services/retrofit/e911/E911ServiceResult.java gov/va/vamf/vavideoconnect/ui/versionawareness/VersionAwarenessViewModel.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ekodevices/library/device/mock/MockWavDevice.java org/fusesource/hawtjni/runtime/Library.java
4	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/fusesource/hawtjni/runtime/Library.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	gov/va/vamf/vavideoconnect/BuildConfig.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	gov/va/vamf/vavideoconnect/hilt/AppModule.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	gov/va/vamf/vavideoconnect/ui/MainActivity.java gov/va/vamf/vavideoconnect/utils/ActivityExtensionKt.java gov/va/vamf/vavideoconnect/utils/UriService.java
00091	Retrieve data from broadcast	collection	com/ekodevices/library/ota/EDOTAManager.java gov/va/vamf/vavideoconnect/ui/MainActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	gov/va/vamf/vavideoconnect/ui/MainActivity.java
00022	Open a file from given absolute path of the file	file	com/ekodevices/ekoconnect/di/StorageModule.java com/ekodevices/library/EDFileHelper.java com/ekodevices/library/device/EDDevice$Companion$decompressAsync$1.java com/ekodevices/library/device/EDDevice.java com/ekodevices/library/ota/EDOTAManager.java com/ekodevices/library/utils/EDBGAutoRecordManager.java com/ekodevices/library/utils/EDCEAutoRecordManager$startRecording$2$1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/ekodevices/library/EDFileHelper.java com/ekodevices/library/device/EDDevice$Companion$decompressAsync$1.java com/ekodevices/library/device/EDDevice$startBulkAssetTransferSendAsync$1.java com/ekodevices/library/device/EDDevice.java com/ekodevices/library/utils/ConvertUtils.java com/ekodevices/library/utils/SignalQualityClassifier.java com/ekodevices/library/utils/ZipDecompressor.java okio/Okio__JvmOkioKt.java org/fusesource/hawtjni/runtime/Library.java
00208	Capture the contents of the device screen	collection screen	org/webrtc/ScreenCapturerAndroid.java
00183	Get current camera parameters and change the setting.	camera	org/webrtc/Camera1Session.java org/webrtc/VVCCamera1Session.java
00056	Modify voice volume	control	org/webrtc/audio/WebRtcAudioTrack.java
00189	Get the content of a SMS message	sms	com/ekodevices/library/device/mock/MockWavDevice.java
00188	Get the address of a SMS message	sms	com/ekodevices/library/device/mock/MockWavDevice.java
00200	Query data from the contact list	collection contact	com/ekodevices/library/device/mock/MockWavDevice.java
00201	Query data from the call log	collection calllog	com/ekodevices/library/device/mock/MockWavDevice.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/ekodevices/library/device/mock/MockWavDevice.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/743887386923/namespaces/firebase:fetch?key=AIzaSyAS5q3dPczbqYTYsNlu1e2g7R_UXh6QwEg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION
Other Common Permissions	7/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FOREGROUND_SERVICE, android.permission.FLASHLIGHT, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
veteran.mobilehealth.va.gov	ok	**IP:** 152.130.100.100 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.903450 **Longitude:** -77.027641 **View:** Google Map
www.veteranscrisisline.net	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
mobile.va.gov	ok	**IP:** 152.130.100.164 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.903450 **Longitude:** -77.027641 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.va.gov	ok	**IP:** 152.130.96.221 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.903450 **Longitude:** -77.027641 **View:** Google Map
dashboard.ekodevices.com	ok	**IP:** 54.86.68.225 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
192.168.1.223	ok	**IP:** 192.168.1.223 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

EMAILS

EMAIL	FILE
this@eddevice.type	com/ekodevices/library/device/EDDevice.java

EMAIL	FILE
video.appointment@va.gov vcc123456789@care.va	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"audio_dialin_enabled_key" : "audioDialInTestingEnabled"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"direct_chat_enabled_key" : "directChatEnabled"
"e911_contact_expiration_time_key" : "e911ContactExpirationTimeMs"
"e911_participant_key" : "E911_PARTICIPANT"

POSSIBLE SECRETS
"e911_participant_name_key" : "E911_PARTICIPANT_NAME"
"e911_result_type_key" : "E911_RESULT_TYPE_KEY"
"e911_transfer_number_key" : "E911_TRANSFER_NUMBER"
"ecrc_number_key" : "ECRCNumber"
"google_api_key" : "AIzaSyAS5q3dPczbqYTYsNlu1e2g7R_UXh6QwEg"
"google_crash_reporting_api_key" : "AIzaSyAS5q3dPczbqYTYsNlu1e2g7R_UXh6QwEg"
"heartbeat_interval_key" : "HeartbeatInterval"
"invite_participant_enabled_key" : "inviteParticipantTestingEnabled"
"pulse_enabled_key" : "pulseEnabled"
"signal_enabled_key" : "silentSignal"
"signal_pull_interval_key" : "SignalInterval"
"vmr_history_conference_key" : "gov.va.vamf.vavideoconnect.vmrHistory_conference"
"vmr_history_name_key" : "gov.va.vamf.vavideoconnect.vmrHistory_name"
"vmr_history_patient_key" : "gov.va.vamf.vavideoconnect.vmrHistory_patient"
"vmr_history_pin_key" : "gov.va.vamf.vavideoconnect.vmrHistory_pin"

POSSIBLE SECRETS
"vmr_history_save_key" : "gov.va.vamf.vavideoconnect.vmrHistory_save"
"vmr_is_transfer_key" : "gov.va.vamf.vavideoconnect.vmr_is_transfer"
"vvc_session_count" : "vvc.session.count"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
CD54FB7B-61A4-40A4-A34A-E6CFEAE11AA6
40B90C02-9306-4DCF-94BD-4CC71515026A
128C9930-5AD6-41FD-BE20-19BE7E82602E
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
00060000-F8CE-11E4-ABF4-0002A5D5C51B
BA9C5360-9999-11E3-966F-0002A5D5C51B
46A970E0-0D5F-11E2-8B5E-0002A5D5C51B
BA0E9DCD-EA10-4AA3-9190-B848598F2F75
C2148E84-CB1F-4A05-9ED0-832A1E9FB336

POSSIBLE SECRETS
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
470fa2b4ae81cd56ecbcda9735803434cec591fa
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
EA73858B-9185-4958-9A7E-7204C3E198E6
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
E6EA3564-D144-4DD3-A884-C9AAA3BFCC19
5BF6E500-9999-11E3-A116-0002A5D5C51B
72BB4346-7487-4552-8779-121DF2435162
7BB44072-14F7-42C2-B0DE-2A340909B180
34696772-1597-429D-A2E3-5C036F9F39DE
2AF120D7-4D40-4FF1-96C6-D803455A3959
600554E8-C6A4-4218-8488-39697AFC7D6A
ba9c5360-9999-11e3-966f-0002a5d5c51b
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3

POSSIBLE SECRETS
93ba7334639c3ef8a750929d70e367cb
41966176-C762-428C-98DA-2A371AAE1C49
B532B98C-7D69-4CDB-B7D0-297A77478790
0aad7ea0-0d60-11e2-8e3c-0002a5d5c51b
5bf6e500-9999-11e3-a116-0002a5d5c51b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
9ebba8238fabbbda48557fae5566b45d
C320D257-D7BE-46AC-9A37-7A4EDFA84BCE
12CAE281-318D-4C0D-A2AF-176639A5C54D
19BE0323-442C-4F80-A0A0-5B7C204FB883
CC719BF7-7AAA-47CE-9CD7-29F223B4B61E
75F0A9DA-183D-4CE6-BC9B-334812D40A1E
00060001-F8CE-11E4-ABF4-0002A5D5C51B

POSSIBLE SECRETS
7BB44072-14F7-42C2-B0DE-2A340909B181
B532B98B-7D69-4CDB-B7D0-297A77478790
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
37C205D6-3D62-43CD-81FB-1E7931950022
C2DE8ABD-959B-4F00-BD84-556A0F45EE28
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
11ec803d7f46828691737a2352fbe71a
00060000-f8ce-11e4-abf4-0002a5d5c51b
32a4f2bd-df39-4885-8d35-a3962372c7c7
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
F1DE0EF3-6E8F-4FA6-B538-5BD318BDBCCB
31DDCAB1-2788-4AF0-B019-9307CEBFAF53

POSSIBLE SECRETS
580B41EC-243F-42D6-A922-8CD6DEF5F941
8CED7DE2-6D15-4E8C-932D-C2BE048146DA
C2D4F30F-E149-43F5-B1B5-B31E7C2EF5D4
dbbb677e84e8eb0efe876620f63ad1d9
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
00060001-f8ce-11e4-abf4-0002a5d5c51b
611CA734-3C3D-4FF7-B908-3587E127DB41
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: VA Video Connect

Score: 4.5 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** gov.va.vamf.vavideoconnect

Developer Details: US Department of Veterans Affairs (VA), US+Department+of+Veterans+Affairs+(VA), None, https://mobile.va.gov/app/va-video-connect, vvc_implementation_team@va.gov,

Release Date: Aug 25, 2021 **Privacy Policy:** Privacy link

Description:

The new VA Video Connect application for Android expands VVC capability to Android users. VVC Android connects Veterans with their health care team from anywhere, using encryption to ensure a secure and private session. The app makes VA health care more convenient and reduces travel times for Veterans, especially those in very rural areas with limited access to VA health care facilities, and it allows quick and easy health care access from Android mobile devices.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:26:57	Generating Hashes	OK
2025-09-01 13:26:57	Extracting APK	OK
2025-09-01 13:26:57	Unzipping	OK
2025-09-01 13:26:58	Parsing APK with androguard	OK
2025-09-01 13:26:58	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:26:58	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:27:00	Parsing AndroidManifest.xml	OK
2025-09-01 13:27:00	Extracting Manifest Data	OK
2025-09-01 13:27:00	Manifest Analysis Started	OK

2025-09-01 13:27:01	Performing Static Analysis on: VA Video Connect (gov.va.vamf.vavideoconnect)	OK
2025-09-01 13:27:02	Fetching Details from Play Store: gov.va.vamf.vavideoconnect	OK
2025-09-01 13:27:04	Checking for Malware Permissions	OK
2025-09-01 13:27:04	Fetching icon path	OK
2025-09-01 13:27:04	Library Binary Analysis Started	OK
2025-09-01 13:27:04	Reading Code Signing Certificate	OK
2025-09-01 13:27:04	Running APKiD 2.1.5	OK
2025-09-01 13:27:07	Detecting Trackers	OK
2025-09-01 13:27:11	Decompiling APK to Java with JADX	OK
2025-09-01 13:27:32	Converting DEX to Smali	OK
2025-09-01 13:27:32	Code Analysis Started on - java_source	OK

2025-09-01 13:27:35	Android SBOM Analysis Completed	OK
2025-09-01 13:27:43	Android SAST Completed	OK
2025-09-01 13:27:43	Android API Analysis Started	OK
2025-09-01 13:27:50	Android API Analysis Completed	OK
2025-09-01 13:27:51	Android Permission Mapping Started	OK
2025-09-01 13:27:59	Android Permission Mapping Completed	OK
2025-09-01 13:27:59	Android Behaviour Analysis Started	OK
2025-09-01 13:28:07	Android Behaviour Analysis Completed	OK
2025-09-01 13:28:07	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:28:09	Email and URL Extraction Completed	OK
2025-09-01 13:28:09	Extracting String data from APK	OK

2025-09-01 13:28:09	Extracting String data from Code	OK
2025-09-01 13:28:09	Extracting String values and entropies from Code	OK
2025-09-01 13:28:14	Performing Malware check on extracted domains	OK
2025-09-01 13:28:15	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.