



ANDROID STATIC ANALYSIS REPORT



 ESET Parental Control (5.3.6.0)

File Name:

ESET Parental Control_merged.apk

Package Name:

com.eset.parental

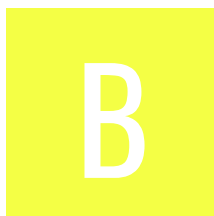
Scan Date:

Aug. 18, 2024, 11:32 a.m.

App Security Score:






48/100 (MEDIUM RISK)

Grade:



Trackers Detection:

1/432

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	37	1	2	2

FILE INFORMATION

File Name: ESET Parental Control_merged.apk

Size: 15.33MB

MD5: 287ca0a88cf342382013814892e97a7b

SHA1: 7ae546b189cd1dbd1f2cab2a854ce140933784e7

SHA256: 86887494c83e97f41880336be51a84fe55bd7c054562c01ade64869bc5a5ca06

APP INFORMATION

App Name: ESET Parental Control

Package Name: com.eset.parental

Main Activity: com.eset.next.startupwizard.presentation.activity.MainActivity

Target SDK: 34

Min SDK: 23

Max SDK:

Android Version Name: 5.3.6.0

Android Version Code: 23503006

APP COMPONENTS

Activities: 17

Services: 16

Receivers: 15

Providers: 3

Exported Activities: 5

Exported Services: 5

Exported Receivers: 7

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=SK, ST=Slovakia, L=Bratislava, O=ESET, spol. s r.o., OU=Mobile application development, CN=ESET, spol. s r.o.
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-04-08 08:40:51+00:00
Valid To: 2038-08-24 08:40:51+00:00
Issuer: C=SK, ST=Slovakia, L=Bratislava, O=ESET, spol. s r.o., OU=Mobile application development, CN=ESET, spol. s r.o.
Serial Number: 0x4d9eca13
Hash Algorithm: sha1
md5: e7edb22d35143205906dc64ed01f1b36
sha1: 65cd9aeb71e2a56e89845f28c63845ac721d56d6
sha256: 0188c3d31232b9f866a0d5342090f875e4318c5d0ad6de83575c0f8d93ea64cc
sha512: b40319a4cbadb045670323b637fc2ff420c8b193ef955f158096fe4cdef0764823f66589b839902a1e682714a1b74f0738d18651cee3d17d81273c2d4e5547d0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: b281418bf85f505f699d0151c8917dff6d8cd1f74a9e1d174042932b1a28a4c
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.
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.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.eset.permission.SMS_TOOL	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_SYSTEM_EXEMPTED	normal	allows system-exempted types of foreground services.	Allows a regular application to use Service.startForeground with the type "systemExempted". Apps are allowed to use this type only in the use cases listed in ServiceInfo.FOREGROUND_SERVICE_TYPE_SYSTEM_EXEMPTED.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.permission.external_app_settings.USE_COMPONENT	signature	permission specific to Huawei devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the Huawei system.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.eset.parental.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check SIM operator check device ID check subscriber ID check possible ro.secure check
	Compiler	r8 without marker (suspicious)
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
classes3.dex	FINDINGS	DETAILS
	Compiler	dx



ACTIVITY	INTENT
com.eset.common.gui.ExternalActionsActivity	Schemes: content://, file://, Hosts: *, Mime Types: application/octet-stream, application/ems, */*, Path Patterns: .*.ems, .*.*.ems, .*.*.*.ems, .*.*.*.*.ems, .*.*.*.*.*.ems, .*.*.*.*.*.*.ems, .*.*.*.*.*.*.ems, .*.*.*.*.*.*.*.ems, .*.*.*.*.*.*.*.*.ems,
com.eset.parental.gui.PageActivity	Schemes: empc://, Hosts: parentalcontrol, Paths: /,



NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------



HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Q MANIFEST ANALYSIS

HIGH: 2 | WARNING: 25 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	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 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.
3	Service (com.eset.commoncore.core.FirebaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Service (com.eset.commoncore.core.accessibility.CoreAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	warning	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.
5	TaskAffinity is set for activity (com.eset.commongui.gui.ExternalActionsActivity)	warning	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.
6	Activity (com.eset.commongui.gui.ExternalActionsActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (com.eset.parental.gui.PageActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.eset.parental.gui.ChildPageActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	TaskAffinity is set for activity (com.eset.commongui.gui.LockSupportActivity)	warning	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.
10	TaskAffinity is set for activity (com.eset.commongui.gui.SimpleLockActivity)	warning	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.
11	TaskAffinity is set for activity (com.eset.commongui.gui.DialogActivity)	warning	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.
12	TaskAffinity is set for activity (com.eset.commongui.gui.FullScreenDialogActivity)	warning	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.
13	Activity (com.eset.parental.gui.recovery.ParentalRecoveryActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity (com.eset.next.main.presentation.ExternalConfigActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (com.eset.parentalcore.core.directboot.DirectBootReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
16	Broadcast Receiver (com.eset.parentalcore.core.broadcast.ChildCoreReceiver) is not Protected. [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.
17	Broadcast Receiver (com.eset.commoncore.core.broadcast.CoreReceiver) is not Protected. [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.
18	Broadcast Receiver (com.eset.commoncore.core.broadcast.AdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.
19	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]	warning	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.
20	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]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	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.
22	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.
23	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.
24	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
25	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
26	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
27	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 2 | WARNING: 9 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	defpackage/e05.java defpackage/e43.java defpackage/fg3.java defpackage/i05.java defpackage/i90.java defpackage/jg5.java defpackage/k80.java defpackage/ky0.java defpackage/nf0.java defpackage/oj2.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	defpackage/lz4.java defpackage/n84.java defpackage/nr4.java defpackage/qn5.java
				defpackage/a47.java defpackage/a86.java defpackage/aa8.java defpackage/ao7.java defpackage/au5.java defpackage/b38.java defpackage/ba.java defpackage/bh0.java defpackage/bt7.java defpackage/c18.java defpackage/c34.java defpackage/co2.java defpackage/cs3.java defpackage/cu1.java defpackage/cy6.java defpackage/d86.java defpackage/da8.java defpackage/do7.java defpackage/dq6.java defpackage/ds3.java defpackage/du5.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/e28.java defpackage/e43.java defpackage/e47.java defpackage/ef8.java defpackage/f18.java defpackage/f62.java defpackage/fc8.java defpackage/ff1.java defpackage/fg.java defpackage/fh7.java defpackage/fl0.java defpackage/fm0.java defpackage/fo0.java defpackage/fy3.java defpackage/fy6.java defpackage/fz5.java defpackage/g18.java defpackage/g43.java defpackage/h14.java defpackage/h74.java defpackage/hf7.java defpackage/hm8.java defpackage/i17.java defpackage/iz3.java defpackage/j17.java defpackage/jg.java defpackage/jg7.java defpackage/jl2.java defpackage/jl3.java defpackage/jl8.java defpackage/jq0.java defpackage/jv.java defpackage/jx.java defpackage/jx1.java defpackage/jx6.java defpackage/jy0.java defpackage/jz3.java defpackage/k17.java defpackage/k18.java defpackage/k57.java defpackage/kc6.java defpackage/kl8.java defpackage/kq6.java defpackage/l37.java defpackage/l78.java defpackage/l93.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	defpackage/l98.java defpackage/ld.java defpackage/ld2.java defpackage/le7.java defpackage/m18.java defpackage/m34.java defpackage/m4.java defpackage/m98.java defpackage/mc8.java defpackage/me7.java defpackage/mf5.java defpackage/mp6.java defpackage/ms3.java defpackage/n17.java defpackage/ng.java defpackage/o17.java defpackage/of0.java defpackage/og1.java defpackage/oj2.java defpackage/oy3.java defpackage/p62.java defpackage/p98.java defpackage/pp0.java defpackage/pu0.java defpackage/pv5.java defpackage/pv6.java defpackage/pw5.java defpackage/q17.java defpackage/q28.java defpackage/q63.java defpackage/r22.java defpackage/r28.java defpackage/rc2.java defpackage/rg.java defpackage/rv2.java defpackage/ry3.java defpackage/s17.java defpackage/s3.java defpackage/s98.java defpackage/sk8.java defpackage/sm8.java defpackage/tj2.java defpackage/tk8.java defpackage/tl0.java defpackage/tl2.java defpackage/tm3.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/u22.java defpackage/u48.java defpackage/u72.java defpackage/u74.java defpackage/uk8.java defpackage/v05.java defpackage/vj8.java defpackage/vk8.java defpackage/vp6.java defpackage/vq7.java defpackage/vy0.java defpackage/wc7.java defpackage/wj2.java defpackage/wn0.java defpackage/wp5.java defpackage/wr3.java defpackage/wv5.java defpackage/x53.java defpackage/x82.java defpackage/xc6.java defpackage/xc8.java defpackage/xf7.java defpackage/xi0.java defpackage/xl8.java defpackage/y37.java defpackage/y74.java defpackage/y82.java defpackage/ya5.java defpackage/yb8.java defpackage/yc.java defpackage/yl3.java defpackage/yr3.java defpackage/z37.java defpackage/zc2.java defpackage/zp0.java defpackage/zr3.java defpackage/zu0.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	defpackage/d65.java defpackage/dl4.java defpackage/hj6.java defpackage/oy6.java defpackage/tp0.java defpackage/wy.java defpackage/z84.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	defpackage/cx3.java defpackage/f95.java defpackage/ha5.java defpackage/hq.java defpackage/kn1.java defpackage/p45.java defpackage/uj1.java defpackage/yx0.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	defpackage/g65.java defpackage/h22.java defpackage/kz0.java defpackage/pt2.java defpackage/rg0.java defpackage/rj7.java defpackage/rp5.java defpackage/t48.java defpackage/vi7.java defpackage/wc5.java defpackage/y0.java j\$/util/concurrent/ThreadLocalRandom.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	defpackage/bx7.java defpackage/lr0.java defpackage/mm6.java defpackage/qu1.java defpackage/t42.java
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	defpackage/i06.java defpackage/k21.java defpackage/kd2.java defpackage/rj7.java defpackage/tr5.java defpackage/v26.java
9	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	defpackage/fw5.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/fw5.java defpackage/iv7.java defpackage/jj0.java
11	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	defpackage/ky0.java
12	MD5 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	defpackage/ky0.java defpackage/kz0.java
13	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	defpackage/r43.java
14	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	defpackage/fz5.java defpackage/y45.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	--------------	-------	-------	---------	---------	------------------

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsprintf_chk', '__memmove_chk']	False warning Symbols are available.
2	arm64-v8a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libparental.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__strncpy_chk', '__strcpy_chk', '__memset_chk', '__strchr_chk', '__strrchr_chk', '__memmove_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>
4	arm64-v8a/libimage_processing_util_jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libcrashlytics.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>No RELRO high</p> <p>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_strlen_chk', '_memmove_chk', '_vsnprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>
6	arm64-v8a/libcrashlytics-trampoline.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>No RELRO high</p> <p>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libcrashlytics-common.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>No RELRO high</p> <p>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsprintf_chk', '__memmove_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>
8	arm64-v8a/libcrashlytics-handler.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>No RELRO high</p> <p>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libparental.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__vsprintf_chk', '__strncpy_chk', '__strcpy_chk', '__memset_chk', '__strchr_chk', '__strrchr_chk', '__memmove_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>
10	arm64-v8a/libimage_processing_util_jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsprintf_chk']	False warning Symbols are available.
12	arm64-v8a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

🚫 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/24	android.permission.READ_PHONE_STATE, android.permission.READ_CONTACTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.VIBRATE
Other Common Permissions	9/45	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE, android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.PACKAGE_USAGE_STATS, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, 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
firebase.google.com	ok	IP: 142.251.37.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.w3.org	ok	IP: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
help.eset.com	ok	IP: 91.228.167.61 Country: Slovakia Region: Bratislavsky kraj City: Bratislava Latitude: 48.148159 Longitude: 17.106741 View: Google Map
accounts.google.com	ok	IP: 108.177.15.84 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
go.eset.com	ok	IP: 20.31.122.183 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
h3-edfdev01-v.eset.com	ok	No Geolocation information available.
smooth-command-782.firebaseio.com	ok	IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
www.epochconverter.com	ok	IP: 188.114.97.10 Country: Spain Region: Madrid, Comunidad de City: Madrid Latitude: 40.416500 Longitude: -3.702560 View: Google Map
www.eset.com	ok	IP: 152.199.21.175 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.034081 Longitude: -77.488503 View: Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	IP: 142.251.37.3 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
suppreq.eset.eu	ok	IP: 20.31.123.179 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
www.youtube.com	ok	IP: 172.217.16.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
maps.google.com	ok	IP: 142.251.36.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
repository.eset.com	ok	IP: 91.228.167.25 Country: Slovakia Region: Bratislavsky kraj City: Bratislava Latitude: 48.148159 Longitude: 17.106741 View: Google Map
ts.eset.com	ok	IP: 91.228.167.155 Country: Slovakia Region: Bratislavsky kraj City: Bratislava Latitude: 48.148159 Longitude: 17.106741 View: Google Map
www.google.com	ok	IP: 142.251.37.4 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	ok	IP: 172.217.16.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
play.eset.com	ok	IP: 91.228.165.68 Country: Slovakia Region: Bratislavsky kraj City: Bratislava Latitude: 48.148159 Longitude: 17.106741 View: Google Map
eset.com	ok	IP: 91.228.166.47 Country: Slovakia Region: Bratislavsky kraj City: Bratislava Latitude: 48.148159 Longitude: 17.106741 View: Google Map
plus.google.com	ok	IP: 142.251.37.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
play.google.com	ok	IP: 142.251.36.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
update.eset.com	ok	IP: 91.228.167.133 Country: Slovakia Region: Bratislavsky kraj City: Bratislava Latitude: 48.148159 Longitude: 17.106741 View: Google Map
pki.eset.com	ok	IP: 38.90.227.50 Country: United States of America Region: California City: San Diego Latitude: 32.715328 Longitude: -117.157257 View: Google Map
login.eset.com	ok	IP: 152.199.21.175 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.034081 Longitude: -77.488503 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	IP: 142.251.37.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
crashpad.chromium.org	ok	IP: 172.217.16.179 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://smooth-command-782.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
export@eset.com	defpackage/pz0.java
test.freeseetlic@gmail.com	defpackage/o31.java

EMAIL	FILE
mobile@eset.com	defpackage/hj0.java
u0013android@android.com u0013android@android.com0	defpackage/mi8.java
export@eset.com	com/eset/customercare/core/domain/handler/a.java
parental@eset.com	Android String Resource

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"endpoint_customer_care_issue_password" : "□□□□□"
"parental_session_leave" : "■□□□□□□□□□□□□□□□"
"Turkey" : "Turcja"
"activation_password" : ""
"Turkey" : "Turecko"

POSSIBLE SECRETS

```
"parental_session" : "□□□□"
```

```
"activation_license_overuse_instructions_link_user": "[u]XXXXXXXXXXXXXXXXXXXXXXXXXXXXX?[/u]"
```

```
"common_username": "000"
```

```
"common_password" : "123456"
```

```
"Turkey" : "000"
```

```
"common_username": "Benutzername"
```

```
"activation_standalone_key_input_label" : "XXXXXXXXXX"
```

```
"common_password" : "סיסמה"
```

```
"customer_care_username": ""
```

```
"com.google.firebase.crashlytics.mapping_file_id" : "86ad31abb1af46d289a1379c16d1a8de"
```

```
"status_parental_session" : "        "
```

"Turkey" : "███"

```
"common_username" : "Username"
```

```
"common_password" : "Senha"
```

```
"google_api_key": "AlzaSyAiCYNi1SqCkhtTU7b9GbvsPIWcuvHuZAE"
```

```
"endpoint_customer_care_issue_password" : "□□□□□"
```

```
"common_password" : "Գաղտնաբառ"
```

"Turkey" : "Turquie"

POSSIBLE SECRETS
"Turkey" : "Turkija"
"Turkey" : "Туреччина"
"common_access_reveal_password" : "□□□□□"
"activation_standalone_key_input_label" : "□□□□□□□"
"Turkey" : "Türkiye"
"activation_license_overuse_instructions_link_user" : "[u]□□□□□□□□□□□□□□[u]"
"parental_session_leave" : "□□□□□□□□"
"parental_session" : "■□□□□□□□□□□□"
"endpoint_customer_care_issue_password" : "■□□□□□□□□□□□□□□□"
"Turkey" : "Թուրքիա"
"common_use_password" : "■□□□□□□□□"
"Turkey" : "Turčija"
"common_password" : "■□□□□□□"
"common_password" : "Heslo"
"history_log_reset_password" : "■□□□□□□□□□□□"
"activation_license_overuse_instructions_link_user" : "[u]□□□□□□□□□□□□□□□?[/u]"
"common_password" : "Geslo"
"menu_user_password" : "■□□□□□□□□□□□□□□□□□□□□"

POSSIBLE SECRETS

```
"common_username" : "██████"
```

"Turkey" : "Турция"

```
"common_username": "0000"
```

```
"common_password" : ""
```

```
"menu_user_password" : "Sicherheitspassword"
```

```
"status_parental_session": "XXXXXXXXXXXX"
```

```
"common_use_password": "123456"
```

```
"activation_username" : ""
```

"Turkey" : "Turquia"

```
"common_password" : "Parola"
```

```
"menu_security_password" : "XXXX"
```

"Turkey" : "Turquía"

"Turkey" : "Turkey"

```
"status_parental_session": "██████████████████████████████████████"
```

```
"menu_admin_password" : ""
```

```
"premium_enter_license_key": "XXXXXXXXXXXX"
```

```
"lock_incorrect_password" : "00000"
```

```
"menu_security_password" : "Sicherheitspassword"
```

POSSIBLE SECRETS

```
"common_use_password": "12345678"
```

```
"google_crash_reporting_api_key" : "AlzaSyAiCYNl1SqCkhtTU7b9GbvsPIWcuvHuZAE"
```

```
"common_access_reveal_password": "████████████████████"
```

```
"common_password" : "Contraseña"
```

```
"premium_enter_license_key": "XXXXXXXXXXXXXXXXXXXX"
```

```
"common_password" : "Wachtwoord"
```

```
"menu_user_password": "0000"
```

```
"common_password" : "Hasło"
```

"Turkey" : "Turcia"

"Turkey" : "ترکيا"

```
"common_access_reveal_password" : "XXXXXXXXXXXX"
```

```
"Turkey" : "███"
```

"Turkey" : "Türkiye"

```
"common_use_password" : "123456"
```

"Turkey" : "Turchia"

```
"history_log_reset_password" : "0000"
```

```
"common_username": "Gebruikersnaam"
```

"Turkey" : "Türkei"

POSSIBLE SECRETS

```
"menu_security_password" : "Beveiligingswachtwoord"
```

"Turkey" : "Τουρκία"

```
"menu_security_password" : "XXXX"
```

```
"firebase_database_url": "https://smooth-command-782.firebaseio.com"
```

```
"premium_enter_license_key" : "00000000"
```

```
"lock_incorrect_password" : "0000"
```

```
"menu_security_password": "████████████████████████████████████████"
```

```
"common_password" : "Password"
```

```
"activation_standalone_key_input_label" : "XXXXXXXXXX"
```

"Turkey" : "Turkije"

```
"history_log_reset_password" : "0000"
```

```
"common_password" : "Parolă"
```

```
"parental_session_leave": "000000"
```

```
"parental_session_leave": "000000"
```

```
"common_username" : "Felhasználónév"
```

```
"history_log_reset_password" : "XXXXXXXXXX"
```

```
"lock_incorrect_password": "████████████████████"
```

```
"premium_enter_license_key": "00000000"
```

POSSIBLE SECRETS

"Turkey" : "Түркия"

"Turkey" : "טורקיה"

```
"common_password" : "Slaptažodis"
```

```
"parental_session": "000000"
```

```
"menu_user_password" : "XXXXXXXXXXXX"
```

"Turkey" : "Törökország"

```
"common_access_reveal_password": "000000"
```

```
"parental_session": "Elternmodus"
```

```
"common_password": "Парола"
```

```
"activation_standalone_key_input_label": "████████████████████████████████████████"
```

```
"status_parental_session" : "        "
```

```
"endpoint_customer_care_issue_password" : "Administratorpassword"
```

```
"common_password" : "Passwort"
```

```
"endpoint_customer_care_issue_password" : "XXXXXXXXXX"
```

```
"common_username": "000000"
```

```
"common_password" : "Jelszó"
```

```
"common_password" : ""
```

```
"common_password" : "Пароль"
```


POSSIBLE SECRETS
"endpoint_customer_care_issue_password" : "Admin-wachtwoord"
"lock_incorrect_password" : "□□□□□□□□□□□□□□"
"parental_session" : "Oudermodus"
"menu_user_password" : "□□□□"
"menu_user_password" : "Beveiligingswachtwoord"
"parental_session" : "□□□□"
"common_password" : "□□□□□"
"menu_security_password" : "□□□□□□□□□□□□"
1161d94817ef782247df151f2459283e691a29cb9bd5f772a372297dbb2ba1b3
8c73007f8a11cd6cd5acb04c2426b831cc2496f8e65041b0ae6056fbfe1c67e0
07163edf59f4abb9edbb0a884b7b4ea802f85b14107ed40d8ca31768d4e84487
969c9f6aaad39fb0337bbe362c2179f3e2d577ac8f89740eef0307e0785efd3e
b8e5ab88-f975-488a-859c-f655504ac81a
7cc722b5-8e33-4547-bbd1-286a383a8b48
a7691f0a-6554-4e72-9334-6ad4d74b75fb
d904ceade3a6f95ab67627ff8d30534849ce48bb8d66c8110f2d7cb450ba6608
927b53b2923c50c066497addcf12b6d7818024decdfb81240e51e988b00571ba
1f694741ac8c78ec659591ef5546bdeff59d9be43551cb6e257d73dca9500a09

POSSIBLE SECRETS
20cedab52a309d9d080c743180203caa32faaf357c4fc57e639379c5db958289
d76497e0e48810aa39bf45faddeb6719ad27360bef00e0792310b404b52a016d
6c49eb902a8c077bbf90f3a0583c135b019a8802d46fac217c945f4b5c96a132
1b63a0af-f4bf-47a6-b32f-d6aef4b86844
c693be9a6a86099ff7f4c7e5fc707edfcfee0cd216960c7ac48bb8410b6f07e4
06aa4840035d2ba792ea3cfe16d1163f8566e6ff78069885887d14b095c80c41
72f880ee-e1e1-4372-a311-bcbe4a9231b0
635c3535d91a48d2d45a7e9c5a7241afc17dfb4d14401d74cb3d2e95222f2eaa
e55ed9b37fe6ebc259e3c9e73ff33a0486b5924fe1a4641cd8ae5d92cc4a7e7b
e12a4eafe9d9163cd90f1c1bedecd871967582b366144e26ea915d0511be512c
c7d35ccb04b8a5b5ce9b2937069bfaebe65822abc04b383339dd1af1e4b2c92
539ec89d9b6f31dcb64db2d374eab63d81040ede4ae12f1a458d90041831e63e
f0a6ed29ee33059e41bafb4304dc899de252ec261a256f4e3917b5231c5601ec
42b255192a7091f02e2c6acdf3881da20ff390e2742691e0901d94c3b48f059f
d7dfaf21c6d29ba7db42966dc4fc1f59f9827353f9049e1b520746ce7d245fbc
41234b6c115032a304e767fd2f29a4ee6f670314dc3098381aeda6b95c7ca5e0
633ed6db35cf7f0d2985bf0c36cc7f322a56cca004284978b27ef7dec7d7bac3
61d61b01e176910f86d276c667e9bed72f9c4c87c2ca886fbc2bfa8e8c3275c6

POSSIBLE SECRETS
f1cedf1a2037e0cd271077b92d4bdecea719737f232d947ed05f3931b9b47c79
9cda762bc0a78065cf5b8baf7bd4c95821754de9c4c788562eea91236c222452
afb8374b3857e2b80efd68c0f3faee66cff30706cbf9da4a718f018516ed6000
262cc6f0c8cf8cbeaad94265630b24218815e4a7415e54c256aca09e03fe1b3b
ffb6bdc0091c965c9bd937ff2f81857f7cb42b799309ca2b9703094e98d3546a
da521a431c5b9792c335c9bb046533c5cc61fa0997215e6703a4b64ba513c357
dd4b80c3506f88b31d37680534598db193c441dbb3fcc07edfb8d3b0b4dd23ea
98a83d0a7270e759e82276ff5ed402ab0d4608f7dc35dd30d490ee9c8aa3ace5
dc1c2db0853111c11f6dac1b44d305fe992c7ca8e4a6a21aa70fbef701bce43b
9938b40c3885f2bb125a1eaa405071fb020306881cbafefb06bf829578a44253
202f71e73f5eff96c3bd2834811aad5c65aff55669bb701a5647c84e7c1582fa
bbfb664e2d82abdaaddfa41ad1061eecedf2e12bec9adfee6dd82ec142f23c9
243abf5ea1fe3f985481447301bc5b7e376b2916afefdeb077c732209e1203b3
a34c5c075b2f0dcd3f356596481ca7572ed444fd85b175a1a6e7ac8b262e59a3
e949938e0cd64670b5ba6dd99d356fe868021bc651d33c66aa461988c8c0298f
793f6ad8e33cdf5bd1d49c1278e80a30f21f62d9416e7f46b4dec0c157b2ae96
52a07761f3e008b520196d76b2f4019838b073d25d909be2a477d90b0b5145d0
4d55b51737513b0e4461823ca4b429039daeea262c03a595906e6861dd31b7a3

POSSIBLE SECRETS
4c3febf0516a8d300c4eb76244da52167d6abcbaf127b3389d1a51efafaa2395
6f0e45eada11fc839dbc5e63949b56507b4e719cc46cb0fab95f796274bf3a8
3c7b7612a9f346f0e85b6b2e2f221aff728c47636eeb01ea8b3c48ebf9413c1e
bcd03c9acd4180d51ca9b83eb4cb94b1148c3af640e4221b5aba6b3121aec4f7
abe5afd51f38657a1803eda59e65cca1e222a26c3147a1bac30a76406b86ce04
721df0128b63125c2560c4c7b02cd6ad2df196385937e4b7de2e02f1f98aaf10
34711679d4b61fa72f4e2b6adce11325783c41bef03929b0140bc02f620d4840
89af5d46f767d0d24a69bc4c1f8136cb70a7d8e79ec1d3f8075a0b5e3326b281
a7bdfdca73504890a0a0625cb360f1dc3d65eb0a4d2d3d8218cc597005997d04
3d8aa1b7c3a1e26f694e4ab6b0f0c4cecf8c61fc1137807a40edd55025dd6b40
717b7a791bacfba3a36ac4d2059ff3aa40f437497f41fc7a3fc72a175f48e498
ec54180cf9eea21443f9c4a9ac72d48dfa7add9867205743891749b7da32b0ae
a9c99d982595d452b152b2333bd4b7963909f82ee8d6d65582070823c528433d
0de5db22-01bf-462c-a633-1b7381a3df29
16677229ba40a13ec1fefb2ccf8f338cdcbe2da4ba6ef81ecfa3244954de0d65
12580547c78dec1adcb4a6a6fb5123c2ab42957420e6d04a69a29c4f31e3ccd1
947ed9d8647248bf7c6cdf3a5ca318c7b7c73ca0a7bedef0545d7449e2b4ff2e
3562d9db1ec20338ded1c450c1831e07a11e5e79aa1647654a3acc9b53ca61dc

POSSIBLE SECRETS
b73a2a52355714cc211821c67ad595d24b8cabae3ace258ffd379b843b891879
3422828a49d0a81a47aee75dbad2a037c3730f4851a8bb445ba683d30a69868a
ba250041-b817-4551-94a9-b08232eb7031
94d7e8621b1cda4d772ac3f30ff78f5e3e85db2c8bba67807a7607f23246deb8
6394ae39ab7f7e9bcd05b61b8d0ef13d185d1074a9c16e46964b4fd374a9126a
3b3f13c6b8975a7f473c0df2ddc553b6ffc2e24bc7fea93bac08f5f2642b8324
f8d8247481885f1c89192b65b37dd7427740012af1e24ded5d2c5cbfcac525fb
45525816bb021e46384453affef1bb962d2c5c7ef0969570681e1c805fe7f80a
ef61a02ea700b486026a38a42780cf38a6c0313fe1674999feaf9102c817f0ac
905bd04b3942b00da73cdca4933fcf1b36dfb507215bc2f0a98fece5241c0e66
118b1777-f6ed-4f24-a8c1-c496f9ec2cac
561cb638ef74da6adc298710fa4d3b88f32e3fe8d5dda8aadf5e4bf50f0983b0
1211531a-d78e-40b0-af2f-58384197b74a
5d3c3ee5482dadd2a39c36880aa70e84559bb9bd3175cc2d933c63eaaaa186d0
d58e590ff06a2463270d49566cb0b70b9f78121294a37ba4737da5e7c1136a94
54d7a56e99eed526cda1fe2190906c6c129e976aa58742f2b76168af47fb5098
08885d80206d97a85c8af94e42b9a609ff201d4b747b37166462263ac40c7013
ee89cb49e2c0a66a4de458d743027f9132e62ab20d64d540454eb266c31620c1

POSSIBLE SECRETS
48d13e860414cd42465202ea68985271a0d856020716cd175cf79f8f98b26e58
877f93d761a56e6fe5441b5c5cf6fc396745129844004d163ab2d641315ce660
2845bf5470c61611add43ad33c0246e19ca1f373a777bb12c31773560ac48335
ddd8c4841667198fec4f9492fdc5eef8c184c8071a9199ec45b6185c5d038747
af74f486bee7224d605594fdcc05b9fb82b6fd84964c59097626a4b7de08d9e7
6ae339b8067d560dbae7e03e13ac3de36081b1c54f246f8cdb6652f96a832ab2
a9c7b6010672735d4bffc29e6d8a901406ddc9299bb09496a73ceb74f0465555
56610410b1a536488ad922f8d1bf2ca58d216417b8754b2dd4bf8a86fb31b549
77de657bcca8853d4d687524f9102b116c0c0c61fe965c3b5fe75f7b1b480a7d
c2993b1f6d2de02e2a285f27e71d1fc7018849178bb2f2617d495272485253e1
8c40c163bad223c96d0d86d894d6d9403cc0beecb75f6d2d9f1129f27856c485
52321887f259549bdf5d4517d970390b7a00ef416f1b40ca2ac1b2504bddcf30
fa9eaeed-0f89-41ce-b935-04fcc8d48d61
61c4e80643f1b990334b61e2af7ebe67d24cf05d5a70651ea822ee40a80a57d9
015234c6472c95efb3e602cd3be07315a1854193cf0b6f82a0ddb90d2d27240d
dd80c0e14308d090aa1e773c8eabcb6616d7472ea9edc928dd6cbcab5a7be7f5
3e3ecdb9a8d1b4fb7c90b3397278675997a9bf7626b557b913aa9c2591f1c118
1feb1bf-b8d3-4715-ae56-b96389b2a241

POSSIBLE SECRETS
508e61a1be85b408007ed3b63cf2af9eeba655da053cf26a693a2e5c2a73e69e
218757f2f90e5eaf19d70fa7f8a0f2a79f48f200a5f1fe38c1f2c7191399a5be
94c6f16525ca8ee13cdf63b23cbcf1300ad08c429d4d24a0b2fb547891dfb0b9
c7fd53ac9c3a0ec019b3db122971f912cd68aeb3361d7ee5538544ed62f5e2fc
18774654648bc011ec6e305ddc5d5d5536261b6a5083ff01fb1f2dfa25b61270
SdH6bgK99F23eCVk21w38qQHLwTcEWo
8c171943739a21339e6aa61616ef945360ccceb65fd8c28fe492ec9143d8521a
3cbd25327b2f1652bc1abd77cc2de55226c0fd530c654fd77679ab049948abcb
ba6467041bc3ff87bbc634d42a38c5961922511c648b4487791b2674e6234f2c
08e15a2265fc1734e0af9b49fc813d4ca5bea8d8a7d83d22845a0c0db6673991
b41fee6aef607c3d6d5fcb60a5a2cf6edd3de86bab9fae69b9e985bcb1a7f82f
7f6612362502af21f89426b76cce59767b2d6cd3cfaf4ada9b16886e2458c2a9
2bc4560a3f212593b572a52cef523ef74cbfa072f63f2f8b5f1223f69cb762f4
9af27dd287431411f856e080648bf20a0ea6b90d3387d61783279e08f316b8f0
ca3c1b56d9279c5e7d32356bce45327eefc8b3b5e0b22c537403f0027da11d63
JNaV6Yvw1vjrZAeth8gtddoxHbxy+OkMfN033Q==
e13ee77b8fff6ac70e6ebcc4c24f122a01e5481380d6f80b5163c9b00d4013aa
f24b2639a53306f9a7ebced217d015aee2858244213e338edaf37d1706195386

POSSIBLE SECRETS
fc4186982a0e39db38777aabf3151752b84b938d0d9c6a33e3b139f2842a31d0
e5e0888f4b20d3c3ee10168d5d312399092ebd58e07c8c2f884c6ce2287d1e01
a112ccd4676d73ab78752d33c562465a6cdd0729d3381aa8aabccfa94ea595cd
51e714d76c8b7bc5b3644af30f79e008d0df9ceb12d585c4b712c3c049a124e1
47d3777a4beba22b9e136b5a55dac3bf269aac22e428ab0fdec22e0646f70299
470fa2b4ae81cd56ecbccda9735803434cec591fa
bf575e89283e049fa64d59412dee35839e38325239e122eb093341784fce3aff
7e4b74419e0252646fdd3ec9b79d9e8183c1a3179688de6c3aea3b418c847ae3
5aaf337b2ddfd2791210ff6db71ccd052c0027ac83fb5a33a38af3d709f83b40
a8edac9589fb0a04ec572baec4e7c537ed7516310f6a122891777cf63f310fae
23bad38b752cf67eefa49e85e5f130a2fbbc6481030669db8f1a0a21c836e57b
96aa78c05c26d2dd888a5760ace4fe076199eb6e76f9461ca370858f1d9a48c7
ad48cdaa9c7ce0c0633f591b466ffecf8fa55e3f9e8f46407d1cc8fc9e33f1dd
e578a20b7b5d10d877ce6fd03bf3d83e674a4dd0d0cf91668c9042ffd28dc1f1
cab8fc7d509f37618d0d10f47f0c1ad0a42e13941d8d087cb8e5f71fd2605b73
b7e187e01fe3ac338aa5af3ee7a3289a1b2223b2b16f6d869585b16fe3e61224
97dc5fbe-c860-4395-a2f2-5ad0a8d74404
b656232b3fa32976258661f68388b858

POSSIBLE SECRETS
cb8108bb0e0a979a4ce338cf1280c33cb3e385572279e9fb0dcffdc24d94a937
205967e16f6b1b350640829322b6418d506cfadc79aa8fe44ee2a9a5e8102f8d
a5427560ccaf940f10682da4d062065899764baa0235313882f7786cdc7a4bad
2e1ab40561050f36a46e1782cae5943f51b76011ea53b2a09de02c47dcc9eaff
a7f30efc2f912c46498e12a0600635467266382775a9f3b44ea09358fd3ffe92
963eb47fe56222e7e2edb2b8d6a4142405799370156d25621eb053bab6b5b203
9506332213571e77ae9d0957186fff4379911f62b83fa27574916d760205305a
6554c8ad9d74565d8708b01fd4bf2b32fe9dad56bb1efb627d0c1d64d9a187bc
aeed376adc819da0ace218959195447c
dfa45094795b90c376c5afc3af53c4e39bab6dc936aab6a29a78719d8b1faae1
283f03cda07a96e457c083164d87dc53713cc4ccf241e337e8404fc9566c5702
aebefa032276dbed14b453f0a5a4211d8fd1675ae3ad8c0242eafe53b85df743
2c8c6c26ded3970283e2e4a98659737d11b942f74cee6fdbbc8dea115fb18b91
86b89548f8f0a69fbbc7324436aed94fb1cb751121bb2a83f3100d0d268b0e9d
99d6cd6de643824c4945bb77dc2b1bb22d69764bf72874777504e4d49663517d
9dc2c644290f5bfcef0d0b310ae963c38ff12975bf90b21a0081fa5e333575c3
8314171502899f0ecb0e5499402c35be99af4dcd1bda1db7e52384bd14dcc64f
0dc8240e-2372-446a-8ef9-97c76570c7ca

POSSIBLE SECRETS
52603d168d4713325545dfcbf9d4abb1766a0d5aa0795f65e538882b6d8d4b86
bce1c4e2-7f69-4b51-b67a-f4333490ba9b
f3555917fdf960b1b6d5e49fe2667f6aeaa0c0e19c6845cd2959bd96a9b1b516
164d8ba434210f0abd6544c5d80fdee664b7612b775d47129d68dd7866a40230
7e1f3b7fe79eefec1250e471faa65f17509357c42357f51c79179ab8c887e646
9dc54300ad9f7078fdef918e913d5e7a80a18ebf58e78aa75f1e069b0aff9c75
3b5fbee1d68b0a2bd5ef2071810112d8de5fcd25613445ef2f8dc66740e5d515
e19cfe926b9022f72a0ec062afbe6806a152cee3ce09fbeb05da2721787f323d
dc159437de1ace34c3dbd713899ffbc3d468cf41b1375ee7c14965e161871816
db550a7fee043a0b0fe8dd09cbe3a1d6cb7cbcf9701a92427328b128653d644d
e52f4bb049644464505d2dc1cc9ea95f2c7778b67190e9b8ad9d998f744395fd
fd9927d7ad5bf66104635806aa2b26f1e24f01613cbcf75286b8be05cd376209
0a3b66f74a5a176859cb16f4195c76f93b7024e23dae37ac19ee6b0756ce4f6a
5c16f8bb0d15bc841fc26b242c50b8da2e41ba99eda04d2f68578078782ecb30
4d435f0d03f23432f89ef007a0bb963dc9dc36c7c181684d5a2ac379928adff0
a5a87d670e61c36a0f1baca4a292f539760ae74f93a769af2e254e8e7c2a5007
85a13eadf8ecc75657a619402fb60491da8d773c2ffb867612a8d296be6bbafa
845441a74a065ceede40dd64bd8fb87c62d2ffb8b7c2be7f033ed81a6cc50533

POSSIBLE SECRETS
50e31062777da60c6bcf624fdd07b39cfd878bbe9bcaf077a50b68bb79cb2e2
673da5b761be444fbd512a38041d89f9d1e7aafce0c684e8ad225507d79cf2b7
4629d22a4484f949cec1c8b2f748a3d0be6b5e1c895ba994aecbc7f679c8932e
b2a6b8d4-5d7f-45a2-90aa-b938a4da73f8
037ba311d8265dbc936a2d6aab54fd215ae3a3f6918b9020c49f59364e5d771e
1a991304d116884f0e890653f576d20afe5a68ade3910c257ecf79e3ee9c4419
8c2310cb394fd2b3227812544ba76534dff683899a33d90faeb2c8adc23b07c5
be154d68c0ec1c96afb39c7c4543e9845e6983a0464379b63c770e7534fbb698
31e55dc0de5fc6ae4c39baaf9c6d516a79fc76e17e70fc5ee5d03e6afa9b959b
e65bd14c1a851165f08898e68c960b5990f63653e23dfaee8a2e193e5b9d4cd4
fa817fa32dc462f6e15f203180006ff3410c1120f8f901fb23bbd08eb571da5f
89e7ba27674248e7198016adc95700b89d57bfd018658b27c662827efb0069ce
ad7086b9329b6859bd277ebe77c018e40a0262178ffa56be2433a5a073927e73
4e97f4a91f4ac0f63c6c5e06982e3b13166a76fe6a36d6032ca5c3a39c64f404
a5d00f708e943bb863cddb45d91ebfd05bd257d26a9629bcda555a65e56a0054
a53120747daf0171b39b2a91bca74eec21378d442210d16606a27c154271f459
5308c3ecfe100e75671c97891a138d9f94c8bd49751eed9a0fed9b6b5de27647
2db2804c345f8c1ad7365918357d94db61981dd4437e7785d68cbe2d8124862a

POSSIBLE SECRETS
d1b641f22ead95cb49e050f76ead4c96b05462ade9619fb23ffb2e59ffbaaf9f
04bbacd9394eda41895502d46a5ac88c9386dc98d5df89e2d95e1943cc9ac018
3cdbf72d29c7bb8d7659c8f3249e4d899f8b998be0fd36b54ab5917a32ff73ce
45c73c71e3b214d8b4f3625f5d21ec63c628c2dce3e04572c5ae55b0e475d9cb
62e63a62bd0923ebd9866c66bf62aded65ca5c1120a112af2f318079d0e66fd0
0846b98cf083c02997dca94f4d9047fdf3646debe04e1d01ec0b41f3de1576e8
0cb38f2d1e59de9f97a4c5df4ccd2e216db10e03a749275808a1b447c75a013c
f3038f94-f5e2-45ac-9f3d-ab25db0f5106
cae49144-8304-4d82-9b43-7f10d62e760a
ef01a0d2f0cac169fa4b290200bb8ff7f4b18cecdb0fddd02b476e8e365b24e5
024d21fae95c1bf66e552ea80811fe4beb669b26f584cd83e93afe61fa122bf
cda329e36afdd89a18ff4fea9806a250129f41b650ee9d12463f014f2ceefa39
729be3c675b90e24641f5fd814729583e191be106e751a0c8b1c987849979585
9857fc45972f2079c7de918a21fa2cdc72ad44301522f8656c8e4f32fe6d531d
7e96ad5cb990682ca74d47e56c7b9d8e9b4277a72efc4222bb86faf952ea7627
391dce6673e1321df822d21acce2bfce4b140fa0c70a16a23d0ef27f5163bde
a43c66e4cf71e041798d2b0a48bd190ca781b2514563e414c265b22b79303d05
ecc5441471de26d9bd1dec73055eb80b61975ba528f7f054e3b509464f17d607

POSSIBLE SECRETS
eefc7dce4cb0f30d7b495714d20a37d9ef399e1ec2ca48aa31f53cc3fb4a0c4c
b48f2b2c9d95b03e0f143f8cf9192c9a1bc6f2cf8f647f0a090960b66109ea8b
4c13faa574420f7ac2fad7fcf676ce54849a7fa7d9ccc6da1e0b046aa04e362c
fca205ee0971ef50e8210bae4b8bfa9e5efad673d083142f4958b7cc7d7a8f0c
3467982714b10c2dd882dc4048a6b3b8132164690178988100f83259bfb7530d
afdd8b9a410ef39a2c0562aa33600126568782e680550392cc44019043523248
f225f19830857551bb9d66e8b5011d4d06644b8be3d1fb3ab6c6f83c6113f0c5
c7ffc5a633db984208ce950cee6e92da9c55a0b18e98380cfc38b7a22adcbda1
f35c1a2a49cff676b392f0412ac2f89ad83500250ac7bf0d7cf82e2ecb4e1527
38926eb05e64e026736121100fdac998b0aa0884d6c83bb76e09be28df300730
1bbab51f7e67be141f5e5eec7d965159f567af98fcbcd51853bcc83dc7f66dec
80eb1a60-cd26-471c-bbaa-e59fe532c108
e70d5b6c87fd83581f453f66afa57158a2e631b923469ec5e530cf50f2ddd31a
15f53315d3350ecf637383f6d9dde56b2534eb86893606bded76ffd31e88f4a6
786a2d0ac99615b0570a5f9e0f310ed0007de953f566fbb050f1ca3d4037f93a
fc5da8647bbea477dc18b8923dba161b9b1ca9fb170fcd080a571588d5317123
5ef6e1d148a89af7525f3c9ac7a2a4eeb7fd88aa9f4c1b08768b571cb1c0bfed
f505b0c3ae9d196a2f4d2ea504550f496e800a15caaf4819384cf6b549cd66d6

POSSIBLE SECRETS
b394b2c4110fbe3118c4720031a87f2b9514c9531c9e076977ca69939a1263ee
fe162ed70bcfc029f51e46ca4f7af473084a2a8be0caa48ccc333a983943cf62
9ba3a4fac6e099cd99f3b0a9073d1a3afa1a4ca1eb5b2682d33574f5241aaad3
e9df3b76024e57cf4fcd45d7cfaaa8fbd95e106613a0d1b0e1884e21b49f9522
2d7c92c18982e3e2f1592ca6163be9ee4fa0f2302fcafd929079f1fe98051d43
7497ac7c4d8d48a7b0efb3d7e9eeea05c1bd993d92cf95140da4d9d4aed70705
8e2f5f366e81caa18f25a1a6d3bf1f09a4001a85de0d136e706a9a44a4b5bc10
45d2d0983103fa05490075da27c031e83676ba91216b04d1fd0d1350cfefc41
8cdeaec9d2752d0a40298383deaf6f1b0a298b946a248188029b12b526b361d9
32c475b75583c12a611bb1b58ef04451549a7b83757e035da8c305556964af5c
33965397be107fd5c4a7437ef4acaf8b159830d94915620b0745717bb7bb40f0
39ec6a394a50693c00eea10b1b778b7faeb25738c7ede1ee60dce6c0298dd325
3767f0a5423596186490514a0062a1946264ed0397e49f0ba1a76cbf30171513
58bd2140d1a0f0a26e56d05dc9ee18565f96eca508b8f76db06a087838e5270a
70fcf12b3b0ea3795013c0d616b66131511dde75891ac25a53fecdd8eaf1cd880
5a20569b-c0fb-4af0-adbe-916c5f736a89
4891a6a6ed2afc8e3163ba84f240d12180bbfcbb9205c400783dc17445ce59ab
3f241b857d6a05f0fb40a77ce4581e9c23d44ad73d00c098f0863b2b0dae2715

POSSIBLE SECRETS
f84ad949fb0ddb541abddeca037c99ea94087fcf166f99e8418b1d336612306f
5b84d1cd5569cfe94ab8220ee44895a6336c8058c4fc42d87a6df21751618e2d
5df923609aa8b82b100e2efe410a5a3cd84995921c8d73aae693d33f21103aa2
42526f7b6da6fbc96a3f4463ef7b7652a995a2b16599ec5367a09da9be3b3a43
17ec105bb8caa0354c8acc901fb20ccf92ea7d42d92bc8c33e1fae612a24e0b2
2a202846d7e2e759d68b3e49f16c93531fdd3618384cf49b4c35ded2f06e02da
e4dd31d917ac3133fb96e2402584ff9c5b7ed197e08f3b883630048c84676fe2
5ec41a84ad4e6310f6f72dbeec3822def403957082b756ff0584a9b152153e249
c56b20a0dab6594254a1d088cd1089d1e983edceb9e35008cf061291f579f4eb
38afc8cafb79616d20165a77be8b2b2fb6e253c1875f84912f7ad516afe7f7fe
35b0335d9e6a9a7039e07b1bb6819680520ee7b8b20523aaeafea03d57936af5
ae135f1f9910ea4d7fa66c8b0bddf1fd364901894b480904964072dbc9e25762
f1aa27089d16db2287249ee4c0e97dd81344911a9b618291c672bccfb3a9317d
3f779afefecc23ae3339a4cb79325fe33116292db658c8e4155b730ff90fcd03
6037714ad4715ea380c6fdc3ca2e7637d50467c1912259f60d5235610c5d2fca
94b95fb9abffdf9b551642ae64859d455b5ca4513e60e57a41373a03c65bc41f
20a03346861347294085b94f81c8b9f8351e38569577184501006a9b2eec6606
6f7dc8a195af505d93ce505e0afac180ee1bb3be5d20f2fe7084c905b11dbc2f

POSSIBLE SECRETS
939a7aa6464435efb7318b918bdf455d5de157542658c42fb3903c2485db41c3
916f10dc517d0a6f16a5c6c4fd5584bc1eb41658119f7cd30f0cd3ef4a90f7c5
0aadb095d18625b437af88dbeaf556ab55ed006ab6ae40ca1894a4f1f9e5cbcb
1d2605e791c33f8a4989ab1c9efc4efda28849e5c7105e2aa261cb7395a8f345
6615f464678fc66d39b28fcf6b3c037a84c49d2cc810b2f04d589d30d5ed90a2
31b1b6e70410d58e1eb04ca0c5b0dd89428eec87135eb9aeb5f213275d630f7b
28842edca53015a6f32dc01e98d628ec0d6a68cfb3efe21a055eb4fdc53a5d7e
3fe2acccf38bfd03626dfc0155892d21f27add644d1a9a0124a791e05da3f5d6
bc94cb9dbc008a2596b611ab03297b8850087cb335d7fdc01e014fea2bfc3500
dec20b0c-54ae-466b-8e9f-39eb8f59387c
fca304ba-9bb9-451c-ac32-0c3276e5c78b
4742dcd0dab69a3d961d02922cd1eb3f4244a28a539571ca4abf8b6b50d46a97
6719fa3f934b1230a3648d4abcc0834e2399458bc4519a790227dd2babcb9dfd
9182f6c3edbe95bd53ec6cdd4d214f047691296c49ccccbda8427cf0caa4c5bd
11e3fc646bef8dbebca31799b27aae8c4836fe24d8e9debda202d193415ad21d
3230a7adf0bf2bfb395a7dfb308047e4233a613914680138d131e753a0c2de1a
f8ca4548-5bba-44f6-954e-3dd8f75e049a
eb56fae58f128745e6890fff4ba0f95939c0b09fa3dfe2a9a91503dfae4623c6

POSSIBLE SECRETS
4ac1d0931071892a31b9927d545a1ca39de208c8485f5b4df4d2b1edbc3d7baf
240726c956caa63acd1697ff303b3e643effab291672abd75baad4c5c80977f7
2398cda033a3827d98a8e6cf1c65d688260271971daa78dad5ed115958d5bf6b
aecbd2332fcee7d9ad79fde8ea718040519a217fc9b100d2786a2cb1a5d7b5dd
6b9e6c4e7cd60314f8f73a1289bec5b7d142236c9c2ff78154b7365e3011fba2
c42012d9785981cf318f18d42a95210c2efebf8b3cb09104ebdc2f69ec44025c
92609d8dafb691f7383a914d205ea40ccb0f4f0bed3aa6b23577c3bc127ff0d3
662b309cec13297970747882d35dbee3
25b52c609b39dce6dd2c425acc375970701635d69617a54e84d5073ee5fc17f8
8f29aba983cc98347ee8d03fc11ec9c1d38abdb9d5b70b25d5efe74a527b1e79
9e51c7a73d43589218826565fbb8d297c416ea85fac807b00868e325248a0422
365c05d9d06559187724fa943ae88256bacfaad06c84afac9984a8ef78cd7e7
0b9afbc667239e2f55c638f10b458a1df3b6b7fe16a0e257a82d9833fda0ea7f
68d7db67e8c78ff5ed1a0d308b636b10de347d0cbcaf768b1ec43419fa1b9232
037b797e11ce1133564d92bf0a10f0b701fc8fbfaed970a9e3811d932438ed9b
6109bd3bf1a8776562a3ec71b4de2914b90833cdd3939cc7eeb32b04ee923e04
4bff42a1a39d85261b78ab238366b866479cff8d9dcbade74a79b5fb56ef393d
79fe9fb3bb0b3f7bd6422240fc75433c3a0ee96cb97742943735ff3b50a35a6b

POSSIBLE SECRETS
b869841bc719aed6333dabc879fcdc841e04ced7e4ea7d8084b78add97c96451
1d81778b34fe196c56abc19cc5b15261cdc54e3e6b0191fd3ea24f7a542f8620
29ef5cad-d7f9-46dc-98ca-599e96ea9a19
d04a199e2056a911d530b6d1cc3bfc8562b1c64f291860221961b62849aae8c3
21920775e99d238149f8a9eac7391b489b90d66fe713087c83283d17d6a32a7d
50094976733d8ebfd25b5b4f208b0256d48188cce3d5ecf9ec741c20ec3d9c65
9ed593db6386a5a11a02238b2982e1ffe18339ffa5d433dbe75eb7a66482447f
a26918af645e7d0a2d53eaf7d2a032941b79e80e3d49c05b79aaf3fa3beff060
41790ac9186fbb06d8cdde50879081e85d20729e692fb9fd87b7cc9182605e34
5e8313f139ce5ae56237b4c5d847e9860b1db2fa9579184883641ed32b1b6169
e0d8a9cb2ee6667d9356a4b1ed416cccbe3a6432d475e1cdf99f03e84afff878
93b24b66101a9ce8427e2782ce864f43330767ca7d737265570724234c7a9f45
a9e8b4cc712a7565e43137a2f43b333d35f8a93eda924accd74c2963babf592a
966eeb293d66cba93d9193ab79ade517a00e53877c1f25ab3f544d2090c99a38
155cc3fdceed80e9e95cdd9295e0c1db677be0d11259ed3a4349182546ec4225
a09d0f1e25f1226260e8ea5ba2afa81be8a2412b408780f7836a6299f97edc7b
55cf59b5610ebf139a2ca8c196c5cd6a4fe17686280d2e0731d613ad2454a352
6dbc33077dcecc7b82ecde5da1021b3ac38cdeeed5041baefd356b9a49127110

POSSIBLE SECRETS
a32e9b8c26d8b361dfd5ee4fe9310f61b52f1d3ec6922b25f17cb65f7eb015d8
26078fa8e56b1771e088be71a626103ccb8118581680c355c78c9f5bb48d0b15
efb79f5eec32d4de3f69c8c59a21f1d77e0205169308fa1a0290012e59d3a9c3
64a110589cdeb3adc3ee9cf58441b87ba874fcd6d9ffc1a39e63b268ddcade
5f4fada8c09532ed5852cdc64d6fb0cd0660f2e85eed12ab4f265a5cdbe82cd
b39369f45ee2ede04228d4b8b1454e7c5fde11de12c79c2cbfd1f85092f06f56
174fbc8cf7766be9e693beb9a49a41e193f1d7cfbdbf324080c3a917eb2f0b5
4f0c3808f770ebd93380bdf2fcba0be41e41e73da06056a47b7a8546ec30886d
aa122d59d04a068534cc2f5671a904d5cbd8e6e837e4e9c1c85f4ed77bf70e37
d9ffc6b9922f1fea050833d6712a6f30267b9b26b3f78366a0f7718eed10ccbb
fc0e1e6a-3f81-4802-8b04-72a56f14317e
23041533a1aa2ee8326e560f260d399548e4e2ad1dabd3c2b89ef81860700952
ea49e1cb55d9f7125b5e46ed66ca6d208cf61d7a7560a093f74b22892f54a0a2
1de8735bbafaabf9cd19c4439a82272a1526d6c9a266f5f2c0b966cb7302783c
7ff891231d010a1af21568cca266cad99bf23a39ba7faf82bd128fd20127d91a
eb9b428eb3cd630e4758e895476352fb102ec615f875d830d29837aebf652c5c
064d70038e56bae474da6607552d8cf8a85853da6a5e3c7c42641f632811b9ac
3c0d3aada373ac9f48befb059fc28b34abde1d23194dc015bfb5d63b36f68543

POSSIBLE SECRETS
f7056b4ae869a5b00e7f82558e55b50d3cfb92aa0696c60707c7e5b3b15dfd0e
e8fbee3e32a7e5efa3dfaa830932ecb312edd66376270b4ccdf9e5574aa35828
e8a7214c56196f563a8cfb6d5f52810bac652e87e3764508945c4bf9f63e5513
60619613fe346374bb873780bf4f81cc6f8efff62c04b421e9c52717e207cb33
a597b432f53e96e988a597b721cc44e8cd1ee2a4ce77697a2d539e87457d76da
1b19134b8189a02e41a25f30a5d0932b1f5bba8e4cf908fef06126b20ca30746
7d73d21f1bd82c9e5268b6dcf9fde2cb
598a315d24077e54db6f8752e81e9b86733da1f1637a0a8a66b44affe2ac5f06
9c6ae37b1929b55bd30f989a3ba0e7a21f574e58f3976297723f4f5b000be01a
82bc99ce12e02e60294c77078ab07c78b64d8c64c9122661227c7abb2227a7ed
db891466c009f20b5e7d558eed944aed4ded2ea8bf697a15d32342b2205835c6
6cdd5376-c6bc-4593-9e88-6d83da0deaa4
76e7143875cf929a0b8d21f4bdd1ee14
19aadf3b21ceca74069bf867876a25063a45d7db658b5080825bc9615eea195b
5fa026665e194d71a3ab3bcab724bf2e544e209a140ddd281c51c589ea16db4f
161e1d12-b61e-4e35-843f-c5f40889073c
e1b482846a08f3846efba12323c691b37efed71e00c3d0197570848950fcb2ed
465774125df35a00c003d8a9f6bbd8ad711cc2870015c16d8e11456befb85d07

POSSIBLE SECRETS
c8c8353d493a71ead1e07d731ed122287745d5785601143299b6c4e1e3dfe320
fa887df28c5959ac531a108637858f6f3fbe2e71c86623d11af9c6e619bf4bf4
a584684982cd05b84870ef9f8be67cc2fe3b71c93e85e75c729704edb209ac64
5161343694a2938d52255e7017e01cf4a0c593e3885afbc9698d857ed9b469c
a977535a442190deb84272bdf3368684bb72ff222204fde0772a90e60cd7d445
8a5752d6b918be227433422b3313f1cdf814b9cb7536965c08f5061716223491
9bfb54e4-2ebb-4b6c-a085-f9082e9a761b
d5a621a29c0c73343cedcc223e9714b0484adca5a8ba64236b075631775607db
184152c518697046d2ccff25283af4d8a5770a74474471ec3f33a8e6ac10900c
3d892a7845570ea39050a63fb80458709e860beee076583fae6469af7f4f0157
8ee9bb598b5416017567f26cc222f1c02327b46b307c3af168fd410c63bbf00e
c9b1e6d56709339dd430a15738e380888faebdce566ecb136e0bed5bb3437bbc
ecae2f5f-542d-415c-b2c1-39425749f3c1
1561d6455b8ee6355ee3ade9aa712f39363f0e3cd5eefffb11c5b093e9b86a5d
9fba41c0674c6540eb95d3bf400b8d9b763e69a590c24c0e833c8380eec88452
9ba6dfd7771bf279c08923183fd0c652e6344912d55bff9b92774d4598930109
7f172d92d8b27ae55df6649f0c4e168b
911ed2385ad4dc999d246f6a8f2410cdc68e944630bf1dfa81cc399c059ae1d9

POSSIBLE SECRETS
ff45adb3b74ed1d903605b2ad04a0052c2b21cd2e0ad841f882545aa5c3c8ed0
d363d903b00f12a0fce18f67488465cc55c786358893cd3ba7951d606c37680a
9c16c4a990455db80df673992722f858da9359c24f47e7f85975b0d403568e05
057598dcf377f1af08e62c3c7bde317e4348e9da549cd2a16b08a1708a1fd959
cfd06be8f612b45d06684bb7a61df05769c690ec692249302deb43d6bbfc9180
27285758426c4a278e9f12eba5331156b47687ee43fffbaae427b3409d0f972e
d16025973aff06f019c8f8aaaddaabe1a0dd81b0241e7f41702091e46e106bc2
8b4d381736d85cc931d18a5187cb0dca7edde36bb188b767a8099b2fee63441f
YW5kcm9pZC5wZXJtaXNzaW9uLklOU1RBTExfUEFDS0FHRVM=
3071c8717539de5d5353f4c8cd59a032
5339c5eff7e5ed6da941679027a218ff751a53b460a78b0650fcae3b40943bb5
8ac3025bcacbf79cd9be76eb09359e4bc79dffde7e5ee4bef3805b030bb77c3b
a5add4cc-91f5-4adb-87f5-2295442e54af
7f069bcd85cc53cd8c1708f471aaf9377f03dd452123bbc7ca28360c971fc06
fb343cebcafb388742087228eba3a59d62d6cee67904c64ee5078969846d9da9
82eb0f70184113a92c6a645b278150ca8a2198213cc8ee4a5cc34fe786e7edf2
ec5cc84ceb86644b4cc772f569a51276aaabd54745138e9cd3c8828139b97880
93057c1405219c73a3a5604eed5da5c44c0cef9bcfc8aa8a0f2a18e613ea4c1d

POSSIBLE SECRETS
97071e7ad6e2568bf504b8a223121bc4af4f65b3b24745867d727877a70a8c3d
7ae5f63f9e06bc53a446ccf1a225daaa9ccf538f9f654cb2e6b26c64f6550456
a194dd6ecc691d482fa8f37c9ff5a42ce4c765eada2f2d67b2873707d303d8cf
7dbe1035527be8aaca86950500590e84de6ec0310ffdd648b0636142030306ac
3e8bfd4973ee47e8c779d00de24b9878976b33afcc20529506aa83e097e325b3
fdf3a112dce4041e38b01eaca48767476fe2255853edb2bf441533c7884a052b
198ba5227d08c22ee5d99507169fc5d80636486408c21ab0edf6fb289b848d3d
c7b8425b13603401e98b909b5eed40b0545552ddf607ce5da8973f1610ec2b30
4bb60fd05b4a03439395ed6c9e6a1db5abc8c37887115b9ca1a23a25860ec4d4
bba8753abf4c6e15c2e618f2c3e2b272f5d882ef26697f1dba756d26818b4e87
0b356a29-f325-40c3-8670-6de077fddb70
067f14f6adb94784dcb40e42d846bb77bb9e62071588f5d3d1528549e04d800d
95644d1291ef453688aa6668a4c4fe07e57e9462095419243534e61eb443741b
5a8b4b6b171d7f9e154295f0f693550710f6dc831da62781e9bc21ab87dc5ceb
9db05664119ddf8834b1c9375df451ca3ceb1b04b484ae70243d47e14bd73336
0a8cff3847b50cbf26e0e61ea9801e223457780ad25b553e6e2a20075e4c153
3ec28e568f45a6d88e742445b9a69f488f0af1efd2251df277bc13538f8e62dd
3374a8a92c0fc08c749204c664c628aa82ba630aa62fe558470e8cf1c3192332

POSSIBLE SECRETS
40884c77f5e1395d8d7175dc586e60f38fb02d29f5ece52caa7fa3695bc57142
2850b3679dc6e6639e2c9c6a9b0089ee0c8a42735b7df94ffea91411e32336ad
99fcaff5fd0ab396d4d71b64ee60288ebe7478916d8d27f037997a2764654b80
3efa489ae4e86bf806dc524ad1c646c4e65421b896dff13e5fddea6a358dcb07
a9abe2ddea256c5841c74bd9c82529bbb4fd0ef314fb3733635c0d5195ff537d
5f80d023cdaea2fafb4500a1ee62a89defa6e241eea7fd9ed2398631f592bec4
bc3941c9430b1278550a3bb70e0d62d31e0577ddff9b82edf7b0e56b6e7d8d68
a1051126-63a2-44a2-b3d4-f1f387517751
2a2317bb88b7ae49bdf71b543bab4a68db7dfb2a6527ceba544d6420345911dc
3f54002e7455a39345249848e8ba4c1d42a2e8d746b3e2ec2ea9fdfe0a4585de
c546199ab36d62ac9372166aa8ab1ef2dc5e4b478d1a71168640cece14a7e143
75d7452c319c6ee730b129602ed4f300055522c10ddf829ef1343cad938b8397
5bf8c56605ca15e4af7a1f4ee6d432030aa592624689f0fd92e165c27fcaf3c6
e0eac8969b35e6d49c1e80deafb04115141bd3483ddd80167554f563aa5ede2c
e517f7d703cbd10773b90ebd7ff30dcae920787065c78113f1434618c1ab0d4b
681f1781b9f12812c830acb1435d0827fd0de3efcb77466c7734ead38abb4414
c007a5bd30a5b6b6d4d240dd3feb7154ad55826115cf7ee51f0a350cc2c6a84a
f6b8a9f09f7f52243f738748cb5fa3d194b5c5dd30039824d651dc53784c2162

POSSIBLE SECRETS
3cc00de1f729737a3dbd4db8167838f28fcbfe3c0b03c14a81805ffad96ed822
9af2f516386251e408e73bed6870b91c5ae52583a541ebecf47d67004bb854e0
245cdf60076cee40a975afff651d57990f61be17de00a7915c7f4eeb9b6e70a9
d149b538c3e5725a7904a4740ab08471a6c83331439d0d4fba1cf6cd7f3412ab
86b2501e81112bf35029d65d938102912fbd62979f4e749c68c13885fe431616
38c587aba88d15fdb77ec4fbf59658c7987f7000f8b99486f013155843036cce
24251eb2331ef43b52bb4fa9f3b780285197a342d338b83e53bdc01688a70fa9
0c6c9b6f8d363e9a4aa3d7e77550792869426d7552e9ed4ece54cc874c033d67
ba9844ba18f72a1d8efcfe4b9c64ab2de99df063a6c241742f2c6632cb704c08
552a79a12907356dcda8d539c587ac57af004ba60bd6d0cb71ae0237b71d6ecb
978b3745-4801-4270-8824-a77ea9db3080
0074ab70-5fe9-45fe-9bce-402c7a7d9305
c2aa64524bd2fa9e302b7b6980ab20f8ae126e1a323daabceedac98015f148e9
a3e30161392622c2b5abeb84c9e328eac264f2b6d356c25aa0732d43ce50fd54
5e2a80a404cfe91c5f56815d597251c530c4ecbcd174d957b88596285d8b0364
b56a21495eb0e087d86d39dc60afdaaadbb24a6c1207d8c0dcd4691d3e263074d
dc8c45642a31c5f4703e41786387004d4913c65e61963e1a2c59bc64a7f048dc
4665812abb885c788c6c007b6db599cc56bde595bbe18ce4dbdfd8b21d1b435b

POSSIBLE SECRETS
e8aa5615-086b-4398-ba20-4a600a3a5f6e
3f3b30a23780dd04350a700bec5c4c8d8fb13ec8822394132f319071d65890d
f9755fd36fdc4be5ba9ea3d2e67bace2b65dc0ceb8bdd34e2e332411df2e52b1
b5b718e7e448b391481c583eeaa40c01c35b04fb7f3528736e115a615aa0f57a
e5a535d77915d455b7ba78df6965eb32ad6a8828883462bef3a4061c69e98dcd
6e0f59fd-3e33-4993-a35f-cf12cb0955e5
acaafa2ff00449c840a7fde3c5e2264b3e1208d4ed4842188df74a0cd88d2078
8d79cd4d576ebf1d3c14d1c0dd082f4ae13b901d7d27f34f3c3a716aaa56c77b
b774172a373805639672714695f6213199368bcd4c39946703006d035a722d79
e369363835a1a3ec4b00b1343a65927558bb15796d9d3a79eebf7f2727990e29
061f0273b5e8ed80c15779b5d5b9774c9bdf1de17ae5fd8d082b1a5b4632ad1b
a2cc023448dddc8720589c0dbc40ae64727be2553941fefcd4668e93e8efe67c
a74dd62302753a779ff3dc340f4fb85dc67f11ff1fad61dce9cee7df77911b96
33b79203-9917-4054-b81e-cb5b22d9aebe
c4c3b5d4e73b517ee1b3299e04f27618d6dbf0c0493873bd21b3d7022efe6c28
f60174553896116cc7d254cd766ab38a4163b685659cb00ffb06575fcfdb6ee0
c73ab20fcaefd9b3ffa9e53303178ce4cd8943b647e4b4acd17ed10dcb8cb118
6d985243b390c14f2f4888d0a0645d7fe0aa758d88ce72293ce2d7c7f697c286

POSSIBLE SECRETS
3be0177cccfdfb46d94e106d8df10a5dbda16f0aef93ecb322644cfdd8e634f6
c2ec997b59648905ea6349183d0498c1df89770ac3be1a0ba9afbc22fcb4e74
c9918c66bec3e2cd7caae0138af888cf96a9ded9c028331225e17de43976157e
1ca28e0477e20c2e26a564d40587049abbb0625e529732e369bfa57e3eaa4b4f
b02b819c1ebbf1f2f8dfda9667de4efbefe86cf15e75d6947dfe09a2e1fdfe72
949c35faeb65acc2fa5706fb4c7a9e0665c0a11be516f954ef863953ec514339
67166f4e0181b71c8c5199ead3b35db562fc3e120ed81f95a8daed1baef3ba33
5c7b652d8560e4ddd047a08a66af8a647de00b97f060c4746383e90517db3be9
40e012ec0bf059f628f57eff14ef30bf494b7d5a22306508a82fec7871b89ed6
f802ce00060c3a0c1f6e6d1d019fb3816dac87f1441e57f7a8bf3c4d2abd5982
aae8a9e71a00635b522b51e9f5d8c27b1e7528621fc9253ace588b77ab5f9980
a5f5e685f1fd0df896db7f0b4390c18615437b99fae662fccce56cc45b4eafc3
7845d2d5981fa6668e4d8dc970753100cadeaf295594025b13f13ea897bc501f
b752af8557bafb60f0904357c2f3c5aea7e31491b04e18c44b1b695c3facf9ee
1afc7214948bdc85653ca5ae6ec3e80e6935ce2f84608afd2b0ea9e419bbf3a5
057595025123473262be7c9289ff788da329d68548999eb9695568396cf8cb3f
e59011140475a265f8024f8d80e3cb829fa8ca3a4f5d68b7e61850242f0532d5
d8pyDHbvrXV5h5FGGrwiWjteb0zZ2Xho

POSSIBLE SECRETS
3e075e1e702fa7d95cfd68cbcb136c4cdb03d31cf95f7c882bae3af9db942fa
09d980db083c985a32b7fabe7e2ed21661b3861e31eb8e344f38da2175804d46
0c814550747f5e2e6746b21c3be5a37cce7ecf0e95c0127c696f3dbb1bdaccff
168bb99e62907ab52766557e61fed5266459dc8be6bb8636a8f88fa4223883dc
f18bc370604e5724befa4d77e3804d3ba6f8446da9a333d1bb9a0b6cb661d9e9
f56b9bd9612e130b888b305d168eef53970351cc057be915ba86a81b89cd3421
728a05af7006df0c0f701b36fad111cb5e96795ffe19a4897ddf8d4ec0a6b41e
43cf0aef4ab75cd3743a27e73a8a40edf412ae3276be5abf38652c9c7136f59
a362749fe715e93cabbc8107833d08f2eeecf2d5220c12f3d0aa8756fc33681
a8b7aa2cb0721b279fbdec78e8edce21dafa237886654a128b9e8358ec7deba1
10d40e89982c7edd7eda371606a668253e63e443cf3e96feb6c246955c7a0720
c0bc5a8293831e7407ce9023bc52e87911d79ed9f950ca6d1feeea4cdcdd54d6
8616c325d6d5946b32cfa7f75a8c5be0df96bf96736b411310f81c7020116234
a3cdc603d0695fc727b4cde3d3718334ac6a716d23e4dad60a0dc9c19c5eab62
c15183e7be4d7d5064db604ca464ec3450705a17264fc4a917be01fa92307eac
a0d497e9-8c7d-4811-a033-0c8201f3b5ee
03a97d0db5c12add8cb3e1d9ee79ace8d911fe3194d662a61936bee541222d2a
feed0277-ee52-4521-aaf0-31438518de2f

POSSIBLE SECRETS
3caf555861aea79ec1986649540a6af6f1efec9ff8418ba5c49a3642022012cb
276295887bafeb3b5c1c98551b55bb7bc88a8cf2a4ab79e1f52b799a364a5608
4afd0a91-7d6d-43de-92af-a8d179a9b0fd
ec7152283f477090f1c4c1b48fdaf13d5a5dac087dbd0d820842182897b58360
a08085fcfdd3ed378878533dfc171c65d2ea4aff6b2af2d41da2f31159d45891
9c407a82bec4b88f88c0d0c27b29a24bd66bcf7481a8aa21e0f1e8df63eb806c
446eb35be82aaab069ff647780b63b766a23a536612b1472e842b54944c4a011
289a670f1e6dd8360b0760cfc59b49d954d63c7d805854bf94dda00f200b48a1
766d3c6732b1de06603b418f1ac6cbb15ff5ccfbe1dae30d2ee8b858e9de988f
9ead97408e91a120fd1e4f33dcf5d8d1d75a176514f582af19a7fe0c24da0c44
00256d009b36445044dd0899b36d9fda39a8867de670955964e0d2ef8b866865
881f79758bb3f70cdc3810c1a3461d3a468ca987b94e95d9a4a938d4bfc72b4f
3dcb94615538551fe0a1e3d9e57e092e1a52cc97a0d1fa3b3d8b5d68465d05bf
7c03e7b1777253e8bb73db1ac9604528c5a7ab12b7f623ed282403b87fb6fe35
ff882d0f58df34d94f52c8704d7f0b942afb9ed8592a72d08b2484d74ed9b8a7
88175e9b65401aed69a9f9682561f44feaf5a00dbe9d6e2609887e7baf43f031
ba75f3582d885b56517a34ac21622743bf1a182629f7f901420257e38aa7451b
e765dae6db2047ba4268ff9bedbda351f7a6abb88d0dc2721399612788e4ff63

POSSIBLE SECRETS
d60229c886494f4112038ce4c4de6b26ac7ab8b6d9bef9ee7fa119ec3643d7d8
65c497762497a85dab103a483a33bbb64949812764e8769fde41d892bb6f5227
4e25deed163dd8e45fc9cc711dcff6db536f839bfaa5bdfa72b9d6e288189ec8
264012d56726f7378b3d627c5bedf9799ad6e0e07a74f694a8f4beefa5ec5d2d
79d8736be494017fa1ccb43d06827fcaef928ae990e1121766ceb368d2f40457
f52bf457d452d1339bb629ac1aa4d3fd6bcd5e23bb84f79661a8a36e3a444f0d
55902cad28feccf32c30aacd39ec9dd38b6255588c85e7810fa84a8eb5ecf0e9
db0d17b98b5dc5c20f5b7a931f4b499fcfe1ccd60b93be35e987f1378c6fa4ca
bd34e43b368467d214593b9214e8655bde7ffd3560d449be7d63e0c2d2b84ba9
af6208bc309e6e04366cb0f9d8118bbe4f1cb8751c80b258588b44f17082f697
ced851900647481e48053224f4d244333f107b6b29a8523befe87dbf3b6a1386
dbda0bd66c373b6848c9da430cf7a8d241aa7839a9f3abcef0d3c7940c0ef425
39ddd13d06ba20165c6023b63904cc882b9b96382bbee5ecc3aa33b0909b1a9b
ef215db6eb9ddfc6a317d999db91a2fe51e1fdcca69b5be0bc8f43d8fe182d14
89749da65e844b56676e804423253f916af8b8c865ac0438d7623ecd8e652c57
21526158a28145a1069e03421cbe1267f2dbbfd74cb781228beabdc64cdf475a
c296f95d3542723206f6fb84aa7c686a4d742325779eee5245e46b383bc83f6d
c2c1e2732c5f2888204e9feb928a4d8960807bcc9cf48e0a26bf4e0acd0db26f

POSSIBLE SECRETS
884566aae150d74b6b27ffc15b65f5ed05aefbab54df27cb6c31c228d224714c
c8265c20a7b3f4948f5230d8a313ca09417441b87e5798beac870261a7022c0c
bb36b3f7ba928a2c007a3548f1395a289031d5896e92876619e491dd1c939702
101b0ab6f20afb78ccf485e4d2da4f758a3e913a31584ecd10665e19b43cb109
0eb62c87d87d113f929393a91e37c52836325d6a2fad8b8f89f44f14a7b22680
905669a34f462643c38e0df152b575257c894a8f62c0b0eabb9523a8ad06494a
706d7210abbdf2fd8681d7520f4a0ac755cb22cbfd0fa3311f1a8bbb3c88d015
782b948e9d6ef4e6b356834ab4b7f7bb94985708575fd8fc3a1bb9ca99faa1c6
5623353189b5e487e21c369491c24014f2f21a994a929e553cd8281d96a65393
b96ad93ebdef404f7ab86c420f7bd7afe879cc5631ea12a9811ae6c2cd433994
6869ff12dff6601e954d4305817aa6cda35ff63ae3b9ec3d58c17a5a69f1b3af
2834cac4fc7737c3b43400817b69b672
9a8c134a-d9d1-43d0-93e2-afb8bc78b72c
98270149d28c77538609d0b84b9d77a4ad5ed8c45036cb1d307c5aeb2e8c6701
d06f1721e1f9265a04e45f009470cfa614394c01ce46451ea49efcae0dfe8e8a
4271e9f06931b7effb7b0bed5d29818994ceac54991059b5fcc8c3e82b4e702e
628a047feb7b3e605f4b8142a67156c91e081938fd5970ecb9420f450d6e98e9
07700907bf272890164074ace3617debe44ca0f22d804b4de47c412842d5f754

POSSIBLE SECRETS
cbced209b9541eb9f3d3adf4065f052ebd725914d06943bd03f1f4eaa096f3e0
0693fd19a3e33dc1678e89dde9e637505ef61524cbff7dea713697d3051bbba6
4e6f82fc55dbe2be21bbc46e8a546b3dfa56f95de637e3605a647bb2b8074ad0
492d3440-693f-43f8-99d1-527b1c5a5c85
1fe79f9da380264f614bb324a1d4e4c311a8f8df0e28691549304ac78947dbd3
162cd7b766baa2599a07c08c115cf67e6c6c70280911bf791b58db8cd2f9646a
563ae8debd927f282301383c1b551c54d30394147926a2fdf15077465f58c25c
b163f85b67792995c7ccee097ceae4936c878191f9c67a5c526deabc67ec8e33
e70ba2b0035376331a20a763dc6370ef518d71b28b6d7b271e87fc75facce92d
e8bafec123645cea60ea9cd54e6728e70e83793932b0aae5d862872c4398df26
454399680944ff17e0ecfd0b07bcb300fc90238381939a80d0f3df4b6fa98c35
e84131753d3399a57c87110ed4fce3ab262d6a0ebad0e3428d2c6bf1dd77db67
5c44ff3f2ffd33b8f68536bf701acf6e8914347b05972c6abc12dc8800391d7b
b42ddfc67317a4e129d59448b6e9ec75aafd8892d7b2141598b1fce40ff66a63
51f1226b899212d3de6d4456611db45517e4d2aee7d6d1b10264fc5291512a7b
71e0ae3d786d8a5129f929d3a89c0df2ee0031765a5463d151786e8e0bd8dc17
9284b60ea37a8a8d0a5dc844cf9ce8c385e89f79c1dc3e976424a22966cb588d
572de1c3fed6d55a9e16640988e48fffc63713bd8a156e850b99de91b6ce5b92

POSSIBLE SECRETS
2016cfc217400f327d3da106ec74e2f7ab9a3063009f91fea55c06d58bb7c701
cbbc29665f5f92bf5d6e0442155ce76eea137c9ccd2f42f7d8631b4c2b37d53b
34591a6abd6dd3ce34d6ee3751baa9ee1cdc296fb2a74e71f69ba81997ba71bd
6423ab6204d0bbaa0ee617577391ece25a527f7142793f477928c56db1a05bc0
18c839b71c9173c8de498a1452e0083407cf967e738b49fd87698f3a2e243dca
9327367cd06183eb69ea59cb51c75aefd0303f2d6ee8c6c2661a8878b274a568
60a14933cc42c8bfa48305a1a8bf8020c23c80a258171261db85110c5f4627a6
49f17ab6e57a94e9580d79d002c93f161cea3eaf14c48ec577d391c6c375a579
d3a8eaad-a8d9-423d-81ae-f6a01deba218
f28b25c9d353d1364fca261f8133f8c777a72eaccd1f748c284af06ae924847b
820e9f71371200121cff015ea7db3079b1c1a9a7053bb4fbb776e3d52253e821
db185b47e8724e272092646f3e78b306a5e65b6f2fc3aba1a13916214a64c5f0
919c0d4eb6e0fd114e1a65b52f69ecaae95bf0a72d86600bd120f91610f56842
7e6bdb4723cc9cc0b3780d275c1ce16a88c064fd8801ec11bb7167e6dba8fb24
28bb4543e3be8618992ea9a2b19f5afb75237c285be792957654908097848c6c
326bb51257686968ddfdb1ea41952e8a5f4d5b60a29738c30daf4e69203adcde
5c53179ac2bbdfe4528a1685057dff5472f6c82f0f4c6b846080ecfc5bb1f04
54cb4aa6aacee90de197f71c4031767c83e34ea5bfb10fca42cd88bc05e8c999

POSSIBLE SECRETS
90d0b888617cf3f6ce86c23e707e59fc1fbbedd12c72c3cbefe1ebb3ad1dd26e
a51ee22f0420d58d78ae4e200fa35afbaab258a6241269842e7e3894867dae14
564ad384aec77d0da427204fb9d246d31ee161ce8f358e3b39003dacbb8f6436
4a7461f6b86aadd45d98891a5ea221ae70576ce62889512e6c8feb8c435517dc
4e19b3299598ddb2484195d7ad3dfd5acb064d666249fe7b4b439058d77b9463
aad7d7e6-a382-4b11-ad8b-096115e7146f
89caf80f4d19b27a6063fa1a607e39f381f54b83f3b08aa3fd9f2b1e1aed60c9
f12c51d4-5b8c-4be9-bfac-74e114c89ab6
47fb58353eb885edf3b41536c484249e4c35da4d391d8f5271b0a14a30207594
9e12d9ecf652f21798ab61a2bf124e2649c3aa681bbb7c771213ccd68a1ad275
cb29ad0f608cd21075a3f91282e4cafe6a309ba8abbf0a603a1b9b26e7884d05
23382f31b41df0e08aa721ed1426fdd123401afcc3fae09cc9f20077fde6ba1e
0f1d95f82b2227bcee923750a8641f2985aba8a636387ef3556c8f7387688a68
1977729c3b55a9d43737b6c1d3740c718015fb570c2ae07ed83ff8a9bdbed31c
6c0fceef3b83e91ccb44912ba11c854289229094b4c91de03591951099508cf1
8e35793f224a61c8f8ebf518685bac2239a3cc8d406123cf200a46026d964568
3f3f3e90a62c2375bfc67cd9d82e3cd4505009bbae364f3f15dfb1d056abb5b9
34e2464195db5c1a0c44f891b367992d9302b12104b63747d61cd1f3c90c355f

POSSIBLE SECRETS
3f94b2aecf6307e491edf827a226433a5401dfc6ab596f4c252f6465c2d20747
97a99dc12343712fe46a94b0697eae1c0132efc5261cdee962989116cec7c509
2a68a606e502c75272174687eb3f3426ca5dfd13d3ce1601564593e40396e39b
d1f53862bc471dddffff40f0758deaeb1598c7e00a1405c083e90fa634024c0a4
e3f05a338f497a9eee4b061c3d8109460a9c7aa2d8e4cb8b1f0f894783efc9c7
9c79bef11b1a8c325ff910ca351374745bacb420144ae8d6b92238ddd5e47d03
4e6d78e8e8107ab18863961496b0098ebdd3b8dc1e88a68073b7dd28185fb71b
191a6878a98f3e4da99733d4035a25a807337048829dd460de200bacc71fa047
06946c3d3df1cfa77aa39e2ec962c3fd1305f7fea0c69297985f08b786c62f21
1e0c6b48b5b6d87fb0795184c2a4b5c3cfde782070757dd4a5f25d23b7fa5884
5a69f867eebfd70e4ca93d9c5df96d51581bf5d8ead265ba5482e827dbeda00d
36cf30b217377641602577193346def1e28eb09df42a87afaeb7fe94898fb498
98e98de3-7745-4171-82ca-dd142ddebc7b
7ac51bd0-af50-424a-8257-169bf1666f07
1ab5b8b4-e715-4d70-a9f1-b913f96c1da4
a912f8027d53cce5903228a49888fc3a4b6c2ef49d3b17d0944203e9177eb509
abc9d6873c862dd8976171cd129ae7050323428d942328758925f73a56300c67
814c15b128e68ad3525ba3d05b0ddd98dae4ee1fe362cc53e823e606e6244e8b

POSSIBLE SECRETS
765a3e0b6e493ab320eae976cb672506bb273e4f73bf97d6b4cfa1102f1f7edb
d28a754a36ee58ac758acc113b818e84ac88cc75c89a1446822807db0b32f950
d97ee40f40d3ca39644ed2940b502dcc4bc146ffd253de8c59efa5f82558e648
ab648e0f7124f93f3459dcca8b6f24929ae0dff5dfd462ddb66567d8a8016ff8
12dd8ebb68fdec1e8465788fc1bcde7d03fb20bba1ab027b12c70f3c9da53812
eb5541f3bdd73e643f4167e3cf774d20c4d09ed111359e9e5ac5075ebe596dad
f2b966ab3d1d8403b088fd44e66f0329a8d46a1dc778431cfeb694580a44777f
627a65bbf69fa23fde9537fb2c0b0e0df7b887249585d7b6d22a03ddb98ef6e2
44bf25cef5189af8a0d9d618caa54b6faa834eb86c7a5046a6cc4ea099e5d0b3
474cbc9dcd65c602fb382c914ba0341885a5d1ffc6451b1c7e1c24d19cc92016
654a469c545388f1723aba665547307f642f56c6bb2b44ed7d107fa2543113e1
fcc5ea4b40c5c6281f860300a908b92bf9bf1c5409dd90e079a166fb76db2c8b
cd0e424ebac37853a5650ef0dc926ab85fe6530a27501437dfca9ec27ab2eb71
1a3c89401959f0e337d6324c0dde570d0b0529781509f92373a0d8d444f5128e
415ef9d39e730f2708dce71f7cb1faaf61bb03e3d4e217c1428ed63f7e0e2cd1
e5d6febd0fa49cdf68ed65a69508f22efce6424f31b4bd2b947e8d46aa90ca1c
694c6eaa0601b2b2666f413b567eaa99d388db34027b1106f6e390590a2e5512
dc77b4eab0725f26ed76252dcc09e12f0aa7708dfa7c6ee5d446967c9bb14df4

POSSIBLE SECRETS
4964f7950c07cbe28bd79ed6565be235e2e2433647e16e9dedaa66bab3b6611b
59604617f020c7a812533e0b541ab54aec62304ac21fa5630cbff285957c3fbf
eb0ecebb87d39b7aab86af808b5db49c
f822887dae642b8c6cc465b0e1e604073e0d25f5bbd7f44cc7ccb1d6d7dd8fc2
1a3a49992881e106d9ace268baaffc3e586ff2326ecb262086bd918e6103f972
f1f2e8938f6940360d3574489f7bac894b94da5f227df8ed52c2133be15d11c3
258c7eb3d108c2acd9b27256380a670c5b2267f1c57a825c8756cb232ea2cd48
35f224a306bb6f8d0f27274afb82bceba5fd7cd7d0b76fc88f69822837f62a9f
1ad31fb118898fcab955d2846e6f4461
edba2dab7878e510b336f060d57da6a4ec11498912663250483569da67eeaf90
300a5e07-d95d-4d34-8640-f9de80575b63
f440bd5bd23b8ef08dcd791e8758ef3dca89ee3714c2b28b25261b88ed549409
99c55bfa91bab12027c5bafa45cba100fc7502ecef7441d66fec66a18e88575
1dd2c34a984efcd133e405840179e08a3cd2ffa7546a690bc640eb29dbb52d22
29907b6456d6f298ad235f72507ef165de0b4a42fde27b16091768e6bdf5e1fa
efc52296-7aef-428b-a187-efda42741b24
0fcc4ad34204c6ed9cb498efbdb7f210da271efc3c999b55ceddaf935ccb1575
7995716c42317adcc8993a6382498870bafc731b062a28e96eca3847716e39f5

POSSIBLE SECRETS
7ec2976c77d7135bfd4f3c1d95c8d21f716e7fd8c2bd1933fbb17ad039a4945e
b0086d4d-1a24-4b17-8ec9-32877c9796dd
aa99d453cab20c13b99e8685b0f3adae1e08f07ecd11483c6dc04bf6ca9cf830
19659b2815484637a8dde265d48db1acee50fd97be581d58659e28a1ff6c0fca
14f9311768ece783ea117fcf45484b187cbb0270007112dd29e6fbf2034726c1
2fba8fbb45c6fdef0ee6b2844712041ae4aa0b4dea85ed7124a388248324272e
0816233ec149e8bc31ba1bf6b120f2822cd1fffde62ad30f7f80aee01e29dcd1
5f180db34bfe2a63b234649421ee638bf4301de7fd009a47f989d4cee9de582a
41ebe9c348b49a085569d74c835fc7e91e26b80296155936fc2682596bfe706f
b76aee97-411e-418a-b76e-39d6f23b2b4a
0cddf38f8d77dd81c6aeb73215b363df5d51b268f0fa73e5da0e125ba1e6a630
7517c66893468c42485754a8a5998d7120c541f2e4918fcf94766bc90b911979
ccfbc7151ec9f50b110c52aebb42175ad6a0a77b6dbe9ffde48b92887f5dab37
2ad7943f-aeff-4213-a1eb-4def69b10402
dcc550e9d46d546714aa5eb72c0d2342d18482dfc71d9dc4aab245b182eee486
14b8b255f52d19c17aff3d6b4d2ed6fbacbacbc90bd123c1d292f7ee348c7830
6bdd8273-3c48-4f73-aabc-82ab7990a677
34b6c1ed1d08f3c13f1089a119924d3197ec545626721870b7dd1172339aed95

POSSIBLE SECRETS
8758be1bbe6c3a40ea613d6447989fd95e8aed220ee5943479ab753be482398e
16c7d34bf51008ac24b899f5cab18e29409b29c8fffc62baf646cbe8f51fcedb
5757264e-7a83-4fd8-8ee9-c3759c135f9e
1e73333560ff1dd9f236311139626731e63b103fa68afb74a7a6f56131f22ee3
07dc53111fb84c96a49f6e4ef15bd62ccc69463f5b7bb2377dc073da9454c274
d9829104046dec2d3c212396927b3f7887a7eb564134e51aaa9de305e7b9d736
cc372503-ac78-4ec6-af6b-53687c0eee2d
c30e17d425472270c3949be876379e879675159ab79905accec52e76435c73e60
3eefc373b8644378ab9ffe7d884ce8c192afbd4743aa4bc826a20e24c3fccd65
b3e7abe825278431ae4c92a34b9da77010799ec7ed6fea15a1483dea1edc16a2
2d4d22f0e7f746f6f16e365ce7a6e0ba555c05d35fb6e5531e21a479022da2fd
c44088860d17d42089520f4e2816de0fe9f1b3d0edbb7de4a72bae25807f76a6
2c4de269-9a6e-4c6e-8b7c-ba4b6c1992a9
776555284038146e2f76d84ea4bedb5363756e734aceb1d64c3bac2150391997
1458d598d9af827cac3fae80c131e8ce18e674394686f35cbe4220878a7fd620
f3db9b70a98ca3f7055e295d477fabcaf9d99af7b43e3113d2f73e67e87d4c54
ccbce2175e15067365d7edab6f14c6ec84ea724c0aa080dcf4a9e76936396795

▶ PLAYSTORE INFORMATION

Title: ESET Parental Control

Score: 3.74 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** Parenting **Play Store URL:** [com.eset.parental](https://play.google.com/store/apps/details?id=com.eset.parental)

Developer Details: ESET, 7608143481226674529, ESET North America 610 West Ash Street Suite 1700 San Diego, CA 92101, U.S.A., <http://www.eset.com>, play@eset.com,

Release Date: Jun 9, 2015 **Privacy Policy:** [Privacy link](#)

Description:

We know how hard it is to set boundaries for your kids on the internet. Our goal is to give you the confidence that they are protected while using smartphones and tablets. 1. Given the opportunity, most kids would be glued to their phones at every waking hour. With App Guard, you can set up the daily limit for gaming and limit playtime at night or during school hours. It automatically controls apps and games and allows kids to use only the age-appropriate ones. 2. When kids are online, they can come across web pages with fake news or violent or adult content. Web Guard ensures your kids' internet safety by keeping them away from inappropriate pages. 3. If your child didn't come from school yet and doesn't pick up the phone, Child Locator locates your child's phone's current location. Additionally, Geofencing allows you to get the notification if your child enters or steps out of the default area on the map. 4. Do you worry about your child's phone's battery dying and not being able to contact them? Set up Battery Protector that will limit playing games if the battery level drops below the default level. 5. Does your child have a crucial task to finish, and you are afraid they will play on their phone instead? Use Instant Block for a temporary ban on games and entertainment. If your child has some free time, you can also temporarily suspend the time limit rule through Vacation Mode. 6. Are the rules too strict? Has a newly installed app been blocked? Children can ask for an exception, and parents can instantly approve or deny requests. 7. Do you want to change the rules settings? Sign in to my.eset.com on a PC or mobile phone and change them remotely. If you, as a parent, also use an android smartphone, install our app on your phone in parent mode, and you will receive instant notifications. 8. Can't reach your kid via phone? Check the Devices section to see if they have turned off the sound or are offline. 9. Do you have kids who have more smartphones or tablets? One license can cover multiple devices, so your whole family is protected. 10. Do you want to know your kid's interests and how long they have spent using their phone? Reports will give you the detailed information. 11. Language barrier? Don't worry, our app communicates with kids in 30 languages. PERMISSIONS This app uses the Device Administrator permission. We can ensure that: - Your children cannot uninstall ESET Parental Control without your knowledge. This app uses Accessibility services. ESET will be able to: - Anonymously protect your children against inappropriate online content. - Measure the amount of time your children spend playing games or using apps. Find more information about permissions requested by ESET Parental Control here: <https://support.eset.com/kb5555> WHY IS THE APP RATING LOW? Please note that children can rate our app too, and not all of them are happy that it can filter content that might be intriguing for them but is wholly inappropriate. HOW TO CONTACT US If you are experiencing any issues with our app, have an idea for how it could be improved, or want to compliment us, contact us at play@eset.com.

☰ SCAN LOGS

Timestamp	Event	Error
2024-08-18 11:32:02	Generating Hashes	OK
2024-08-18 11:32:02	Extracting APK	OK

2024-08-18 11:32:02	Unzipping	OK
2024-08-18 11:32:02	Getting Hardcoded Certificates/Keystores	OK
2024-08-18 11:32:04	Parsing AndroidManifest.xml	OK
2024-08-18 11:32:04	Parsing APK with androguard	OK
2024-08-18 11:32:05	Extracting Manifest Data	OK
2024-08-18 11:32:05	Performing Static Analysis on: ESET Parental Control (com.eset.parental)	OK
2024-08-18 11:32:05	Fetching Details from Play Store: com.eset.parental	OK
2024-08-18 11:32:06	Manifest Analysis Started	OK
2024-08-18 11:32:06	Checking for Malware Permissions	OK
2024-08-18 11:32:06	Fetching icon path	OK
2024-08-18 11:32:06	Library Binary Analysis Started	OK
2024-08-18 11:32:06	Analyzing lib/arm64- v8a/libcrashlytics-common.so	OK

2024-08-18 11:32:06	Analyzing lib/arm64- v8a/libcrashlytics-handler.so	OK
2024-08-18 11:32:06	Analyzing lib/arm64- v8a/libparental.so	OK
2024-08-18 11:32:07	Analyzing lib/arm64- v8a/libimage_processing_util_jni.so	OK
2024-08-18 11:32:07	Analyzing lib/arm64- v8a/libcrashlytics.so	OK
2024-08-18 11:32:07	Analyzing lib/arm64- v8a/libcrashlytics-trampoline.so	OK
2024-08-18 11:32:07	Analyzing apktool_out/lib/arm64- v8a/libcrashlytics-common.so	OK
2024-08-18 11:32:07	Analyzing apktool_out/lib/arm64- v8a/libcrashlytics-handler.so	OK
2024-08-18 11:32:07	Analyzing apktool_out/lib/arm64- v8a/libparental.so	OK
2024-08-18 11:32:09	Analyzing apktool_out/lib/arm64- v8a/libimage_processing_util_jni.so	OK
2024-08-18 11:32:09	Analyzing apktool_out/lib/arm64- v8a/libcrashlytics.so	OK
2024-08-18 11:32:09	Analyzing apktool_out/lib/arm64- v8a/libcrashlytics-trampoline.so	OK
2024-08-18 11:32:09	Reading Code Signing Certificate	OK

2024-08-18 11:32:09	Failed to get signature versions	CalledProcessError(1, ['/jdk-20.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/287ca0a88cf342382013814892e97a7b/287ca0a88cf342382013814892e97a7b.apk'])
2024-08-18 11:32:09	Running APKiD 2.1.5	OK
2024-08-18 11:32:11	Detecting Trackers	OK
2024-08-18 11:32:13	Decompiling APK to Java with jadx	OK
2024-08-18 11:32:29	Converting DEX to Smali	OK
2024-08-18 11:32:29	Code Analysis Started on - java_source	OK
2024-08-18 11:32:51	Android SAST Completed	OK
2024-08-18 11:32:51	Android API Analysis Started	OK
2024-08-18 11:33:08	Android Permission Mapping Started	OK
2024-08-18 11:35:54	Android Permission Mapping Completed	OK
2024-08-18 11:35:56	Finished Code Analysis, Email and URL Extraction	OK
2024-08-18 11:35:56	Extracting String data from APK	OK

2024-08-18 11:35:57	Extracting String data from SO	OK
2024-08-18 11:35:57	Extracting String data from Code	OK
2024-08-18 11:35:57	Extracting String values and entropies from Code	OK
2024-08-18 11:35:59	Performing Malware check on extracted domains	OK
2024-08-18 11:36:02	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.

© 2024 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).