ANDROID STATIC ANALYSIS REPORT

Family Safety (1.26.2.1015)

File Name:	base.apk
Package Name:	com.microsoft.familysafety
Scan Date:	Aug. 11, 2024, 3:04 p.m.

App Security Score:	53/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	37	2	2	1

FILE INFORMATION

File Name: base.apk
Size: 55.41MB
MD5: 672a0c830a00261952445683f332e567
SHA1: 5c7eb4df48aa7096e7be7a19b480d1328eebf83a
SHA256: 73b68a82db3dc910629222bd9e45418acc2eae356a3575f86314f65232710a8d

APP INFORMATION

App Name: Family Safety
Package Name: com.microsoft.familysafety
Main Activity: com.microsoft.familysafety.MainActivity
Target SDK: 33
Min SDK: 26
Max SDK:
Android Version Name: 1.26.2.1015
Android Version Code: 401015

APP COMPONENTS

Activities: 11
Services: 21
Receivers: 41
Providers: 2
Exported Activities: 1
Exported Services: 5
Exported Receivers: 18
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft Family Safety for Android, CN=Microsoft Corporation Third Party Marketplace (Do Not Trust)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-02-13 18:56:24+00:00
Valid To: 2034-09-30 18:56:24+00:00
Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Corporation Third Party Marketplace PCA
Serial Number: 0x33000000fec6b802f6654f3cc80000000000fe
Hash Algorithm: sha256
md5: d7fd0e178bdfd491e8edcc880288b176
sha1: dfbbf68b028706619d8dfcfd8cfb8c2314535651

```
sha256: 382497aa856f5c984c23bce9a97f4dbcd442f1e39f46a92ca78b23c82caaea58
sha512: 6c01bba005247885978e0f0f1d1725e2fd59ec1c769bde7e25cb4f8c3f1b89a0a4693be6216bd3f5f51de0fcff77266273bffb2a7177fdc67a9711c3597542bc
X.509 Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Corporation Third Party Marketplace PCA
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2010-10-08 23:15:35+00:00
Valid To: 2034-10-08 23:25:35+00:00
Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Corporation Third Party Marketplace Root
Serial Number: 0x61362ca7000000000002
Hash Algorithm: sha256
md5: 8439748a4d2c09e95e2b8acdab653c6d
sha1: 155d434f0e34f140a795a4864a2531133e528f3a
sha256: b17e8201b128e1e74cc023510ab7ea03ac27dde50d32d810ea1577758f1cc098
sha512: e690ef1bec86d5b150baf5e467e5c116bd4b8c1ea84d8866c0bdff30fa43184756f9a991d76147a053e68854e641175fe7254d8a7002ea2bfd1769c7fbd824c8
X.509 Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Corporation Third Party Marketplace Root
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2010-10-05 22:02:28+00:00
Valid To: 2035-10-05 22:09:33+00:00
Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Corporation Third Party Marketplace Root
Serial Number: 0x33959c19504871914238df73d3b49a3d
Hash Algorithm: sha256
md5: bc7de72f3fe2e0645233efb9917c6bcd
sha1: 05861fde0ccacd6eec8d91db6e0f22c257748532
sha256: 2848361a9c1e32df1d3e2ed6a7b9e67a525cf8a13b164f8006c9479578f746de
sha512: 9c8d6a8c11333ac88ded91bccdfc04790233a2af58dacc9a636b7b1b66f5b35f7d6622c3330615a8b105a6c0a933421e0f3b3b00f5a2753847f31a2e0a28b090
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: f25b8f3ea60ffd1119c19d141d3b0ebad001bb7b41e0a6d4e1454d945ce7fb71
Found 3 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.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.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.HIGH_SAMPLING_RATE_SENSORS	normal	Access higher sampling rate sensor data	Allows an app to access sensor data with a sampling rate greater than 200 Hz.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.microsoft.familysafety.MainActivity	Schemes: familysafety://, https://, http://, Hosts: @string/fmc_base_url, Path Patterns: /family/settings/content-filters/.*/web, /family/settings/content-filters/.*/apps, /family/settings/spending/.*, /family/settings/screen-time/.*/apps, /family/settings/screen-time/.*/devices, /family/settings/overview/.*,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **26** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
3	TaskAffinity is set for activity (com.microsoft.familysafety.screentime.pip.PictureInPictureActivity)	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.
4	Service (com.microsoft.familysafety.screentime.services.FamilySafetyAccessibilityService) 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	Service (com.microsoft.familysafety.core.pushnotification.FirebaseCloudMessagingService) 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.
6	Broadcast Receiver (com.microsoft.familysafety.core.broadcasts.UninstallAppReceiver) 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.
7	Broadcast Receiver (com.microsoft.familysafety.screentime.admin.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.
8	Activity (com.microsoft.appcenter.distribute.DeepLinkActivity) 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	Broadcast Receiver (com.microsoft.appcenter.distribute.DownloadManagerReceiver) 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.
10	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.
11	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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Broadcast Receiver (com.sentiance.sdk.BootCompletedReceiver) 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.
13	Broadcast Receiver (com.sentiance.sdk.TimezoneChangeReceiver) 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.
14	Broadcast Receiver (com.sentiance.sdk.location.LocationProviderChangeReceiver) 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.
15	Broadcast Receiver (com.sentiance.sdk.DebugReceiver) 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.
16	Broadcast Receiver (com.sentiance.sdk.task.ConnectivityChangeReceiver) 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.sentiance.sdk.task.PowerStateChangedReceiver) 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.sentiance.sdk.deviceinfo.UpgradeBroadcastReceiver) 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.
19	Broadcast Receiver (com.sentiance.sdk.activitytransition.ActivityTransitionChangeReceiver) 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.
20	Broadcast Receiver (com.sentiance.sdk.movingstate.MovingStateTimeoutReceiver) 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.
21	Broadcast Receiver (com.sentiance.sdk.movingstate.StationaryAssistantReceiver) 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.
22	Broadcast Receiver (com.sentiance.sdk.autostopdetection.SdkDetectionTimeoutReceiver) 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.
23	Broadcast Receiver (com.microsoft.beacon.network.WifiStatusReceiver) 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
24	Broadcast Receiver (com.microsoft.beacon.services.BootReceiver) 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.
25	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.
26	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.
27	Service (com.evernote.android.job.gcm.PlatformGcmService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.

CODE ANALYSIS

HIGH: **0** | WARNING: **8** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/gifdecoder/c.java com/bumptech/glide/gifdecoder/d.java com/bumptech/glide/load/data/a.java com/bumptech/glide/load/data/c.java com/bumptech/glide/load/data/e.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/cache/c.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/f.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/s.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/a.java com/bumptech/glide/load/model/g.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/a.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/c.java com/bumptech/glide/manager/d.java com/bumptech/glide/manager/g.java com/bumptech/glide/manager/h.java com/bumptech/glide/request/SingleRequest.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/util/pool/FactoryPools.java d2/c.java d2/e.java d4/k.java d5/d.java e4/p.java e4/q.java f2/g.java f2/h.java g2/a.java h4/a.java i2/a.java i2/d.java l2/c.java l2/j.java l2/k.java l2/r.java l2/t.java net/time4j/base/d.java org/tensorflow/lite/NativeInterpreterWrapper.java p2/a.java p2/c.java p2/h.java r2/a.java s2/c.java s3/j.java si/a.java t3/f.java t3/r.java t5/g.java t5/l.java t5/m.java v2/h.java v5/b.java v5/c.java x3/l.java yh/b.java z1/b.java z1/e.java
2	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	b7/c.java b7/e.java com/evernote/android/job/f.java com/microsoft/appcenter/persistence/a.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/microsoft/connecteddevices/AFCDataAceessLayer.java com/microsoft/powerlift/android/internal/db/OpenHelper.java com/sentiance/sdk/events/g.java com/sentiance/sdk/payload/submission/a.java o7/d.java w0/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/microsoft/powerlift/android/internal/sync/IncidentPersister.java j8/d.java
4	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	aa/c.java aa/d.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/l.java com/bumptech/glide/load/engine/q.java com/microsoft/appcenter/channel/b.java com/microsoft/beacon/location/CurrentLocation.java com/microsoft/cll/android/h.java com/microsoft/familysafety/contentfiltering/db/models/ContentRestrictionEntity.java com/microsoft/familysafety/contentfiltering/db/models/WebRestrictionEntity.java com/microsoft/familysafety/core/auth/k.java com/microsoft/familysafety/database/f.java com/microsoft/familysafety/features/db/models/RemoteFeatureEntity.java com/microsoft/familysafety/safedriving/crashdetection/SafeDrivingCrashReport.java com/microsoft/familysafety/safedriving/e.java com/microsoft/familysafety/spending/SpendingInsights.java com/microsoft/maps/MapUserPreferences.java com/microsoft/maps/MapView.java com/microsoft/powerlift/PowerLiftClient.java com/microsoft/powerlift/android/PartnerAppLogUploadReceiver.java com/microsoft/powerlift/android/internal/db/IncidentInfo.java com/microsoft/powerlift/android/internal/db/UploadInfo.java jb/b.java jb/c.java od/a.java org/bondlib/Throw.java pa/a.java ta/a.java
5	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	com/microsoft/appcenter/http/g.java com/microsoft/cll/android/EventQueueWriter.java com/microsoft/cll/android/t.java com/sentiance/sdk/location/a.java com/sentiance/sdk/task/e.java ig/a.java ig/b.java jg/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	com/microsoft/powerlift/PowerLiftClient.java com/sentiance/sdk/task/e.java t5/h.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/microsoft/powerlift/android/http/CertPinningHttpClientFactory.java ei/e.java ei/f.java pd/c.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	d5/r.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/microsoft/connecteddevices/DeviceProperties.java
10	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	com/microsoft/connecteddevices/DeviceProperties.java ve/f.java
11	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/microsoft/familysafety/spending/BottomSheetWebView.java com/microsoft/powerlift/android/RemedyActivity.java
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	l8/d.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	x86_64/libBingMaps-MapControl.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.	Full RELRO info 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.	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: ['__vsnprintf_chk', '__read_chk', '__memmove_chk', '__strlen_chk']	False warning Symbols are available.
2	x86_64/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full 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.
3	x86_64/libc++_shared.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.	Full RELRO info 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.	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	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libcdp_one_sdk_android.1.5.0.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.	Full RELRO info 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.	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.
5	x86_64/libBingMaps-MapControl.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.	Full RELRO info 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.	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: ['__vsnprintf_chk', '__read_chk', '__memmove_chk', '__strlen_chk']	False warning Symbols are available.
6	x86_64/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full 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	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libc++_shared.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.	Full RELRO info 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.	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.
8	x86_64/libcdp_one_sdk_android.1.5.0.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.	Full RELRO info 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.	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.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	8/45	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.PACKAGE_USAGE_STATS, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.ACTIVITY_RECOGNITION, 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
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
activity.windows.com	ok	**IP:** 20.44.229.112 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
location.family.microsoft.com	ok	**IP:** 20.166.139.158 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
auth.xboxlive.com	ok	**IP:** 52.143.85.83 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
account.live.com	ok	**IP:** 13.107.42.22 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
dev-powerlift-frontdesk.acompli.net	ok	**IP:** 40.119.12.22 **Country:** United States of America **Region:** Texas **City:** San Antonio **Latitude:** 29.424120 **Longitude:** -98.493629 **View:** Google Map
android.notify.windows.com	ok	No Geolocation information available.
global.notify.windows.com	ok	**IP:** 20.199.121.23 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.p9.sentiance.com	ok	**IP:** 3.220.73.205 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
cs.dds.microsoft.com	ok	**IP:** 20.82.217.86 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
prod.support.services.microsoft.com	ok	**IP:** 104.40.214.227 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
api.sentiance.com	ok	**IP:** 63.33.87.45 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
powerlift.acompli.net	ok	**IP:** 13.107.246.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.bingmapsportal.com	ok	**IP:** 20.50.64.12 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
peoplehub.xboxlive.com	ok	**IP:** 2.18.68.8 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
account.microsoft.com	ok	**IP:** 2.17.245.241 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map
olmprodpowerlift-cdn.azureedge.net	ok	**IP:** 13.107.246.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
in.appcenter.ms	ok	**IP:** 4.152.45.235 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
maps.google.com	ok	**IP:** 142.251.39.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sas.office.microsoft.com	ok	**IP:** 13.107.246.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dev-powerlift-gym.acompli.net	ok	**IP:** 13.107.246.44 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
activity.microsoft.com	ok	No Geolocation information available.
privacy.microsoft.com	ok	**IP:** 2.17.245.133 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map
xapprove.xboxlive.com	ok	**IP:** 52.184.246.154 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
settings.data.microsoft.com	ok	**IP:** 51.104.136.2 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.microsoft.com	ok	**IP:** 2.18.69.217 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xsts.auth.xboxlive.com	ok	**IP:** 52.156.147.113 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
sisudemo.azurewebsites.net	ok	**IP:** 52.183.82.125 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
s.dnet.xboxlive.com	ok	No Geolocation information available.
olmdevpowerlift-cdn.azureedge.net	ok	**IP:** 13.107.246.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
aad.cs.dds.microsoft.com	ok	**IP:** 20.82.217.86 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
sisu.xboxlive.com	ok	**IP:** 20.69.192.122 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
mobileaggregator.family.microsoft.com	ok	**IP:** 20.223.13.196 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
s.xboxlive.com	ok	No Geolocation information available.
user.auth.xboxlive.com	ok	**IP:** 20.99.128.106 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.bingapis.com	ok	**IP:** 13.107.5.80 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
go.microsoft.com	ok	**IP:** 2.18.38.33 **Country:** Argentina **Region:** Ciudad Autonoma de Buenos Aires **City:** Buenos Aires **Latitude:** -34.613152 **Longitude:** -58.377232 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdpcs.microsoft.com	ok	**IP:** 20.54.232.160 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
ohanaandroid-cd45d.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.bing.com	ok	**IP:** 95.101.23.169 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
microsoftedgewelcome.microsoft.com	ok	**IP:** 20.40.24.37 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
plus.google.com	ok	**IP:** 142.250.201.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fd.dds.microsoft.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
bing.com	ok	**IP:** 13.107.21.200 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
ppe.activity.windows.com	ok	**IP:** 52.142.19.2 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
login.live.com	ok	**IP:** 20.190.177.85 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
powerlift-frontdesk.acompli.net	ok	**IP:** 51.107.58.163 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
www.tensorflow.org	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.251.208.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
continuum.dds.microsoft.com	ok	**IP:** 20.82.217.86 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
vortex.data.microsoft.com	ok	**IP:** 20.189.173.7 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
cdpcs.access.microsoft.com	ok	No Geolocation information available.
img-prod-cms-rt-microsoft-com.akamaized.net	ok	**IP:** 95.101.75.46 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
safedriving.family.microsoft.com	ok	**IP:** 20.166.139.211 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
location.microsoft.com	ok	**IP:** 13.107.6.158 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
aka.ms	ok	**IP:** 23.3.110.134 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
accounts.xboxlive.com	ok	**IP:** 20.72.200.55 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
bn2-df.notify.windows.com	ok	**IP:** 20.199.121.23 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
appassets.androidplatform.net	ok	No Geolocation information available.
family.microsoft.com	ok	**IP:** 2.17.245.241 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
support.microsoft.com	ok	**IP:** 2.17.244.108 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
arc.msn.com	ok	**IP:** 20.223.35.26 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
dev.virtualearth.net	ok	**IP:** 13.107.246.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
mobile.events.data.microsoft.com	ok	**IP:** 51.105.71.137 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
sas3.office.microsoft.com	ok	**IP:** 13.107.246.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xboxlive.com	ok	**IP:** 20.70.246.20 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://ohanaandroid-cd45d.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238
Sentiance		https://reports.exodus-privacy.eu.org/trackers/290

HARDCODED SECRETS

POSSIBLE SECRETS
"ending_session" : "Zakończenie Session"
"ending_session" : "Ending Session"
"ending_session" : "■■■■■■■■ ■■■■■"

POSSIBLE SECRETS
"ending_session" : "Rematando sesión"
"ending_session" : "Terminando Sessão"
"ending_session" : "Saioa aixten"
"ending_session" : "סיום Session"
"ending_session" : "□□□□ Session"
"google_api_key" : "AIzaSyC44ecVG3pBVFjEI9tHewQ6EoDF3LCHqsE"
"sos_session_ended_msg" : "□□□□□□□□□□□□□%s□□□□□□"
"ending_session" : "■■■■■■■ ■■■■■■■"
"ending_session" : "Завршна Сесија"
"firebase_database_url" : "https://ohanaandroid-cd45d.firebaseio.com"
"ending_session" : "Lýkur lotu"
"ending_session" : "Užbaigiamas seansas"
"ending_session" : "Fine sessione"
"ending_session" : "Afslutter Session"
"ending_session" : "Munkamenet befejezése"
"ending_session" : "Oturum Sonlandırılıyor"
"ending_session" : "Završna Sesija"
"ending_session" : "Завершение сеанса"
"ending_session" : "Avsluttar økt"
"ending_session" : "Završetak Sesije"
"ending_session" : "Mengakhiri Sesi"

POSSIBLE SECRETS
"ending_session" : "Končanje seje"
"ending_session" : "□□□□ □□"
"google_crash_reporting_api_key" : "AIzaSyC44ecVG3pBVFjEI9tHewQ6EoDF3LCHqsE"
"ending_session" : "Avslutar Session"
"ending_session" : "Tamat Sesi"
"ending_session" : "Avslutter Økt"
"ending_session" : "Završetak sesije"
"ending_session" : "إنهاء الجلسة"
"ending_session" : "Päätetään istuntoa"
"sos_session_ended_msg" : "■■■■■■■■■■■■■■■■■■■■■■■■■%s■■■■■■■■■■■■■■■"
b5d15d4b-695a-4cd5-93c6-13f551b310df
e-3034d91e-5efa-9fbe-1384-46009f087ccf
69e7f8d4769f4b9a811daa5e59c6c70d-f898824d-053f-4dac-a6fd-d2d76c04bb8d-7686
f4365e74007243479e86bd1a77c49912-eccf3d30-3b47-4752-b4ba-9d999ea969b7-6734
b3e97e8fc4df33ec153b7bb26869039ae0e5a474
cc80ee4401ae9d91cb3c01129e7699cf
ABCDEFGHJKMNPQRSTUVWXYZ23456789
BOhGq12lOTdAWvspc0LzW8RISDWPdnhLdLAGSVz
50838ec0f7f62cc93a66a862f9296f41
59867dae421f422b87c201e5b89b6898-989893cc-c14e-4e0d-a00f-451c8dddf5ef-7399
-11-e0edbbfb-cfc5-4011-868b-2ce77ac7c70e

POSSIBLE SECRETS
-c6951746-8ee5-8461-0809-fbd755cd902e
c3b65c7208d140a7bca3f36b7b0b334a
41edfaa8639ea04bfdc4acba338708e51d8754f01bd969459dab64b08cb4ede8cae692ea01e246e37b806aa03517b50609a3859fdb62d717279aa52cb12a91bc
f61754ff1afb40b48fa24fbbc2b2b7ba
c103703e120ae8cc73c9248622f3cd1e
5d4586dc289ba10600003231
445b9e24-0ea4-4f82-ad0c-9d49205b00f3
93993C5BAC99776BBFA9EDBB9A1EC2069B727BAF
a7898e0f-ea9a-487a-b015-1e4d964e46de
-2d0764e1-5ec5-f6a1-6898-0bc18f71e318
5e4d717b1680cc0600000002
4435fcd8-8d0a-4247-9b4f-6e546f3c148f
dce5010f-c52d-4353-ae86-d666373528d8
mH5wS05CAaZg+IDEQYOCxvaGBMm3LEpW
49f946663a8deb7054212b8adda248c6

PLAYSTORE INFORMATION

Title: Microsoft Family Safety

Score: 3.891258 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Parenting **Play Store URL:** com.microsoft.familysafety

Developer Details: Microsoft Corporation, 6720847872553662727, One Microsoft Way, https://www.microsoft.com/en-us/microsoft-365/family-safety, FamilySafetyFeedback@microsoft.com,

Release Date: Jul 17, 2020 **Privacy Policy:** Privacy link

Description:

The Microsoft Family Safety app helps empower you and your family to create healthy habits and protect the ones you love. Get peace of mind that your family is staying safer while giving your kids independence to learn and grow. This app is designed for both parents and kids. For parents, it helps to create a safe space for their children to explore online. Set parental controls to filter inappropriate apps and games and set browsing to kid-friendly websites on Microsoft Edge. Help your kids balance their screen time activity. Set limits for specific apps and games on Android, Xbox, or Windows. Or use device management to set screen time limits across devices on Xbox and Windows. Use activity reporting to better understand your family's digital activity. View your kids' activity in a weekly email to help start a conversation about online activity. For kids, it ensures their safety in the digital world by adhering to parental controls and accessing age-appropriate content. Microsoft Family Safety features: Activity reports – Develop healthy digital habits • Activity log of screen time and online usage • Weekly email summary report of activity Screen time – Find a balance • Screen time app and game limits on Xbox, Windows, Android • Screen time device limits on Xbox and Windows • Get notified if your child requests more time Content filters – Explore safely • Web filters for kid-friendly browsing on Microsoft Edge • Block inappropriate apps and games Privacy & Permissions Your privacy is important to us. We work around the clock to protect your data and information to help you keep your family safe. For example, we do not sell or share your location data with insurance companies or data brokers. We provide you with meaningful choices about how and why data is collected and used and give you the information you need to make the choices that are right for you and your family. With your child's consent, Microsoft Family Safety may collect interaction data using accessibility, app usage, and device admin service permissions. This allows us to: know when they are using an app, exit an app on their behalf, or block apps that are not allowed. Disclaimers This app is provided by either Microsoft or a third-party app publisher and is subject to a separate privacy statement and terms and conditions. Data provided through the use of this store and this app may be accessible to Microsoft or the third-party app publisher, as applicable, and transferred to, stored and processed in the United States or any other country where Microsoft or the app publisher and their affiliates or service providers maintain facilities.

☰ SCAN LOGS

Timestamp	Event	Error
2024-08-11 15:04:14	Generating Hashes	OK
2024-08-11 15:04:14	Extracting APK	OK
2024-08-11 15:04:14	Unzipping	OK
2024-08-11 15:04:15	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 15:04:20	Parsing AndroidManifest.xml	OK
2024-08-11 15:04:20	Parsing APK with androguard	OK
2024-08-11 15:04:24	Extracting Manifest Data	OK
2024-08-11 15:04:24	Performing Static Analysis on: Family Safety (com.microsoft.familysafety)	OK
2024-08-11 15:04:24	Fetching Details from Play Store: com.microsoft.familysafety	OK
2024-08-11 15:04:25	Manifest Analysis Started	OK

2024-08-11 15:04:25	Reading Network Security config from network_security_config.xml	OK
2024-08-11 15:04:25	Parsing Network Security config	OK
2024-08-11 15:04:25	Checking for Malware Permissions	OK
2024-08-11 15:04:25	Fetching icon path	OK
2024-08-11 15:04:25	Library Binary Analysis Started	OK
2024-08-11 15:04:25	Analyzing lib/x86_64/libBingMaps-MapControl.so	OK
2024-08-11 15:04:27	Analyzing lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:04:27	Analyzing lib/x86_64/libc++_shared.so	OK
2024-08-11 15:04:29	Analyzing lib/x86_64/libcdp_one_sdk_android.1.5.0.so	OK
2024-08-11 15:04:32	Analyzing apktool_out/lib/x86_64/libBingMaps-MapControl.so	OK
2024-08-11 15:04:34	Analyzing apktool_out/lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:04:35	Analyzing apktool_out/lib/x86_64/libc++_shared.so	OK
2024-08-11 15:04:36	Analyzing apktool_out/lib/x86_64/libcdp_one_sdk_android.1.5.0.so	OK
2024-08-11 15:04:39	Reading Code Signing Certificate	OK
2024-08-11 15:04:40	Running APKiD 2.1.5	OK

2024-08-11 15:04:45	Detecting Trackers	OK
2024-08-11 15:04:50	Decompiling APK to Java with jadx	OK
2024-08-11 15:05:58	Converting DEX to Smali	OK
2024-08-11 15:05:58	Code Analysis Started on - java_source	OK
2024-08-11 15:07:05	Android SAST Completed	OK
2024-08-11 15:07:05	Android API Analysis Started	OK
2024-08-11 15:07:57	Android Permission Mapping Started	OK
2024-08-11 15:08:38	Android Permission Mapping Completed	OK
2024-08-11 15:08:43	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 15:08:43	Extracting String data from APK	OK
2024-08-11 15:08:47	Extracting String data from SO	OK
2024-08-11 15:08:47	Extracting String data from Code	OK
2024-08-11 15:08:47	Extracting String values and entropies from Code	OK
2024-08-11 15:08:53	Performing Malware check on extracted domains	OK
2024-08-11 15:09:05	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.