MOBSF

ANDROID STATIC ANALYSIS REPORT

Lawnchair (2.0-2589)

File Name:	Lawnchair_2.apk
Package Name:	ch.deletescape.lawnchair.plah
Scan Date:	March 2, 2022, 4:30 a.m.
App Security Score:	**42/100 (MEDIUM RISK)**
Grade:	B

FINDINGS SEVERITY

HIGH	⚠ WARNING	INFO	✓ SECURE
9	29	2	2

FILE INFORMATION

File Name: Lawnchair_2.apk
Size: 6.96MB
MD5: 0f5c8a70eaae9c99ab53714c924ee8da
SHA1: 510aa699e8b73f3679965f82b682694d935220d3
SHA256: 6d7da6ba8ed10e5acdfed5a1c9f4c973972ec99015dba209afa3f67db44234a2

APP INFORMATION

App Name: Lawnchair
Package Name: ch.deletescape.lawnchair.plah
Main Activity: ch.deletescape.lawnchair.LawnchairLauncher
Target SDK: 28
Min SDK: 21
Max SDK:
Android Version Name: 2.0-2589
Android Version Code: 2589

APP COMPONENTS

Activities: 28

Services: 6

Receivers: 7

Providers: 7

Exported Activities: 13

Exported Services: 3

Exported Receivers: 6

Exported Providers: 6

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: False

Found 1 unique certificates

Subject: CN=Till Kottmann O=Deletescape Media

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2017-07-03 06:48:05+00:00

Valid To: 2042-06-27 06:48:05+00:00

Issuer: CN=Till Kottmann O=Deletescape Media

Serial Number: 0x1bd97ec7

Hash Algorithm: sha256

md5: b12e96be16ae8ba05422410447728647

sha1: 9590bdf21fc8b54d2557211a8bdbcfb41160894b

sha256: 47ac92631c603513cc8d26dd9cffe0719a8b365544dccec2095824ec256120a7

sha512: bf2231fc5489260bf3384fc44f2e09c55343965a164ce93f2b96ca363d0fda3f462e1ec53ba3c5ce359de0b6e97e3d7b2309a75785a130299f7a99526a277f5f

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 60fd01bf315ed487c8533930ddf492f61f0cba3c273d22aeff4d27da0cc916cb

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.launcher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.WRITE_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
ch.deletescape.lawnchair.plah.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
ch.deletescape.lawnchair.plah.permission.WRITE_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.CONTROL_REMOTE_APP_TRANSITION_ANIMATIONS	unknown	Unknown permission	Unknown permission from android reference
com.google.android.apps.nexuslauncher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.apps.nexuslauncher.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
ch.deletescape.lawnchair.plah.permission.QSB	unknown	Unknown permission	Unknown permission from android reference
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.SET_WALLPAPER	normal	set wallpaper	Allows the application to set the system wallpaper.
android.permission.INSTALL_SHORTCUT	normal		Allows an application to install a shortcut in Launcher.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.READ_WALLPAPER_INTERNAL	unknown	Unknown permission	Unknown permission from android reference
android.permission.DEVICE_POWER	signature	turn phone on or off	Allows the application to turn the phone on or off.
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.
com.android.permission.RECEIVE_LAUNCH_BROADCASTS	unknown	Unknown permission	Unknown permission from android reference
com.huawei.wallpaperservcie.permission.SET_WALLPAPER_OFFSET	unknown	Unknown permission	Unknown permission from android reference
com.huawei.android.thememanager.permission.ACCESS_CHANGE_WALLPAPER	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.LAUNCHER_ANIMATION	unknown	Unknown permission	Unknown permission from android reference
com.inveno.hwread.permission.LAUNCHER_RECEIVE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BIND_ACCESSIBILITY_SERVICE	signature		Must be required by an AccessibilityService, to ensure that only the system can bind to it.
android.permission.REQUEST_DELETE_PACKAGES	normal		Allows an application to request deleting packages.
android.permission.BIND_APPWIDGET	SignatureOrSystem	choose widgets	Allows the application to tell the system which widgets can be used by which application. With this permission, applications can give access to personal data to other applications. Not for use by common applications.
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.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.REMOVE_TASKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.REAL_GET_TASKS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_FRAME_BUFFER	signature	read frame buffer	Allows application to read the content of the frame buffer.
android.permission.GET DETAILED TASKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_INSTANT_APPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_ACTIVITY_STACKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.START_TASKS_FROM_RECENTS	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.CREATE_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.FORCE_STOP_PACKAGES	signature	force-stop other applications	Allows an application to stop other applications forcibly.
android.permission.MANAGE_DEVICE_ADMINS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_SECURE_SETTINGS	SignatureOrSystem	modify secure system settings	Allows an application to modify the system's secure settings data. Not for use by common applications.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
org.pixelexperience.weather.client.READ_WEATHER	unknown	Unknown permission	Unknown permission from android reference
ch.deletescape.lawnchair.plah.permission.BROADCAST_BUGREPORT	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
xyz.paphonb.systemuituner.permission.MODIFY_NAVBAR	unknown	Unknown permission	Unknown permission from android reference
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.SET_WALLPAPER_HINTS	normal	set wallpaper size hints	Allows the application to set the system wallpaper size hints.

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.

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.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
<tr><td>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
ch.deletescape.lawnchair.backup.RestoreBackupActivity	Schemes: file://, content://, Hosts: *, Mime Types: application/vnd.lawnchair.backup, application/octet-stream, application/x-zip-compressed, application/zip, */*, Path Patterns: .*\\.shed, .*\\..*\\.shed, .*\\..*\\..*\\.shed, .*\\..*\\..*\\..*\\.shed, .*\\..*\\..*\\..*\\..*\\.shed, .*\\..*\\..*\\..*\\..*\\..*\\.shed, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.shed, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.shed, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.shed,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	api.openweathermap.org	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Content Provider (com.android.launcher3.LauncherProvider) is not Protected. [android:exported=true]	high	A Content Provider 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.android.quickstep.TouchInteractionService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.STATUS_BAR_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	Activity (com.android.quickstep.RecentsActivity) is not Protected. [android:exported=true]	high	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
6	Content Provider (com.android.quickstep.LauncherSearchIndexablesProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.READ_SEARCH_INDEXABLES [android:exported=true]	warning	A Content Provider 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.
7	TaskAffinity is set for Activity (ch.deletescape.lawnchair.settings.ui.SettingsActivity)	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.
8	Activity (ch.deletescape.lawnchair.settings.ui.SettingsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
9	Activity-Alias (ch.deletescape.lawnchair.settings.ui.SettingsLauncherActivity) is not Protected. An intent-filter exists.	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Activity (com.google.android.apps.nexuslauncher.search.AppLaunchActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
11	Broadcast Receiver (com.google.android.apps.nexuslauncher.qsb.OPAStatusReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.CAPTURE_AUDIO_HOTWORD [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.
12	Broadcast Receiver (com.google.android.apps.nexuslauncher.smartspace.SmartspaceBroadcastReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
13	Content Provider (com.google.android.apps.nexuslauncher.search.AppSearchProvider) is not Protected. [android:exported=true]	high	A Content Provider 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
14	Activity (ch.deletescape.lawnchair.backup.RestoreBackupActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
15	Activity (ch.deletescape.lawnchair.settings.ui.SettingsIntegrationActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
16	Activity (ch.deletescape.lawnchair.iconpack.ApplyIconPackActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
17	TaskAffinity is set for Activity (ch.deletescape.lawnchair.iconpack.EditIconActivity)	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.
18	Activity (ch.deletescape.lawnchair.gestures.LawnchairShortcutActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
19	TaskAffinity is set for Activity (ch.deletescape.lawnchair.gestures.ui.RunHandlerActivity)	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.
20	Activity (ch.deletescape.lawnchair.gestures.ui.RunHandlerActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
21	Activity (ch.deletescape.lawnchair.FakeLauncher) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
22	Broadcast Receiver (ch.deletescape.lawnchair.gestures.handlers.SleepMethodDeviceAdmin$SleepDeviceAdmin) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Service (ch.deletescape.lawnchair.LawnchairAccessibilityService) 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.
24	Content Provider (ch.deletescape.lawnchair.FiveSecsProvider) is not Protected. [android:exported=true]	high	A Content Provider 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.android.launcher3.InstallShortcutReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.android.launcher.permission.INSTALL_SHORTCUT protectionLevel: dangerous [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. However, the protection level of the permission is set to dangerous. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
26	Broadcast Receiver (com.android.launcher3.SessionCommitReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
27	Broadcast Receiver (com.android.launcher3.AppWidgetsRestoredReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
28	Service (com.android.launcher3.notification.NotificationListener) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.
29	Activity (com.android.launcher3.dragndrop.AddItemActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
30	Activity (ninja.sesame.lib.bridge.v1.access.RelayActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
31	Activity (ninja.sesame.lib.bridge.v1.access.BeaconActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
32	Content Provider (ninja.sesame.lib.bridge.v1.access.CommandProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
33	Content Provider (ninja.sesame.lib.bridge.v1.access.IconProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/deletescape/lawnchair/touch/WorkspaceOptionModeTouchHelper.java ch/deletescape/lawnchair/smartspace/MediaListener.java com/bumptech/glide/Glide.java ch/deletescape/lawnchair/smartspace/OnePlusWeatherDataProvider.java ch/deletescape/lawnchair/globalsearch/providers/web/WebSearchProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/hoko/blur/opengl/functor/DrawFunctor.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/manager/RequestManagerFragment.java ch/deletescape/lawnchair/LawnchairBugReporter.java ch/deletescape/lawnchair/customnavbar/CustomNavBar.java ch/deletescape/lawnchair/settings/ui/GridSizeDialogFragmentCompat.java ch/deletescape/lawnchair/touch/PinchStateChangeTouchController.java com/hoko/blur/opengl/offscreen/OffScreenBlurRenderer.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/util/pool/FactoryPools.java ch/deletescape/lawnchair/settings/ui/SettingsActivity.java ch/deletescape/lawnchair/gestures/handlers/SleepTimeoutActivity.java com/bumptech/glide/load/engine/Engine.java ch/deletescape/lawnchair/iconpack/DynamicDrawable.java net/oneplus/launcher/OPWeatherProvider.java ch/deletescape/lawnchair/animations/SplashResolver.java ch/deletescape/lawnchair/animations/AnimationType.java ch/deletescape/lawnchair/backup/LawnchairBackup.java ch/deletescape/lawnchair/bugreport/DogbinUploadService.java ch/deletescape/lawnchair/bugreport/BugReportClient.java com/bumptech/glide/request/SingleRequest.java com/topjohnwu/superuser/internal/InternalUtils.java ch/deletescape/lawnchair/settings/ui/HighlightablePreferenceGroupAdapter.java com/hoko/blur/opengl/offscreen/EglBuffer.java com/hoko/blur/processor/OriginBlurProcessor.java eu/chainfire/librootjava/Logger.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java ch/deletescape/lawnchair/predictions/LawnchairEventPredictor$logShortcutLaunch$2.java me/jfenn/attribouter/fragments/AboutFragment.java ch/deletescape/lawnchair/preferences/SmartspaceEventProvidersAdapter.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.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	ava ch/deletescape/lawnchair/bugreport/BugReportClient$connection$1.java com/bumptech/glide/manager/SupportRequestManagerFragment.java ch/deletescape/lawnchair/font/CustomFontManager.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java me/jfenn/attribouter/data/github/GitHubData.java com/hoko/blur/util/ShaderUtil.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java ch/deletescape/lawnchair/LawnchairApp.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/hoko/blur/processor/NativeBlurProcessor.java ch/deletescape/lawnchair/blur/BlurWallpaperProvider.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java ch/deletescape/lawnchair/gestures/handlers/StartVoiceSearchGestureHandler.java com/bumptech/glide/load/model/ResourceLoader.java ch/deletescape/lawnchair/settings/ui/search/SearchIndex.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/manager/RequestManagerRetriever.java ch/deletescape/lawnchair/colors/ColorEngine.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java ch/deletescape/lawnchair/iconpack/IconPackImpl.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/hoko/blur/opengl/functor/ScreenBlurRenderer.java com/bumptech/glide/gifdecoder/GifHeaderParser.java ch/deletescape/lawnchair/smartspace/SmartspacePixelBridge.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/hoko/blur/task/BlurTaskManager.java ch/deletescape/lawnchair/smartspace/LawnchairSmartspaceCont

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/deletescape/lawnchair/smartspace/LawnchairSmartspaceController.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/RequestBuilder.java ninja/sesame/lib/bridge/v1/access/IntegrationActivity.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java ch/deletescape/lawnchair/blur/BlurWallpaperProvider$updateWallpaper$2.java com/bumptech/glide/load/engine/executor/GlideExecutor.java ch/deletescape/lawnchair/adaptive/IconShape.java ch/deletescape/lawnchair/smartspace/OWMWeatherDataProvider.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ByteBufferEncoder.java me/jfenn/attribouter/wedges/Wedge.java ch/deletescape/lawnchair/smartspace/WeatherIconProvider.java ch/deletescape/lawnchair/LawnchairIconLoader.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java ch/deletescape/lawnchair/LawnchairPreferences.java ch/deletescape/lawnchair/gestures/GestureController.java ch/deletescape/lawnchair/iconpack/AdaptiveIconCompat.java ch/deletescape/lawnchair/theme/ThemeManager.java ch/deletescape/lawnchair/twilight/TwilightManager.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java ch/deletescape/lawnchair/gestures/handlers/StartGlobalSearchGestureHandler.java ch/deletescape/lawnchair/gestures/handlers/StartAssistantGestureHandler.java ch/deletescape/lawnchair/adaptive/AdaptiveIconGenerator.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/hoko/blur/opengl/program/Program.java ch/deletescape/lawnchair/gestures/handlers/LaunchMostRecentTaskGestureHandler$onGestureTrigger$1$$special$$inlined$let$lambda$1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	ch/deletescape/lawnchair/LawnchairBugReporter.java ch/deletescape/lawnchair/backup/LawnchairBackup.java ch/deletescape/lawnchair/settings/ui/DecorLayout.java
3	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	eu/chainfire/librootjava/Policies.java eu/chainfire/librootjava/Logger.java eu/chainfire/librootjava/RootIPC.java eu/chainfire/librootjava/Reflection.java ch/deletescape/lawnchair/root/RootHelperManager.java eu/chainfire/librootjava/IRootIPC.java eu/chainfire/librootjava/RootIPCReceiver.java eu/chainfire/librootjava/RootJava.java eu/chainfire/librootjava/AppProcess.java ch/deletescape/lawnchair/root/RootHelperManager$ipcReceiver$1.java ch/deletescape/lawnchair/root/RootHelper.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	ch/deletescape/lawnchair/LawnchairLauncher.java ch/deletescape/lawnchair/allapps/PredictionsDividerLayout.java ch/deletescape/lawnchair/bugreport/BugReportService.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/deletescape/lawnchair/smartspace/accu/AccuRetrofitServiceFactory.java com/kwabenaberko/openweathermaplib/implementation/OpenWeatherMapHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	ch/deletescape/lawnchair/bugreport/BugReportService.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	lib/arm64-v8a/libhoko_blur.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libhoko_blur.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libhoko_blur.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86_64/libhoko_blur.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['bluetooth', 'network connectivity', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
12	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
15	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
16	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
jfenn.me	ok	**IP:** 172.67.194.73 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
avatars1.githubusercontent.com	ok	**IP:** 185.199.108.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.qwant.com	ok	**IP:** 194.187.168.100 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 172.217.166.164 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bumptech.github.io	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
suggest.yandex.com	ok	**IP:** 213.180.204.63 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
openweathermap.org	ok	**IP:** 138.201.197.100 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
api.iplocate.app	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.github.com	ok	**IP:** 20.205.243.168 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
geoip-db.com	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
del.dog	ok	No Geolocation information available.
www.startpage.com	ok	**IP:** 37.0.87.15 **Country:** Netherlands **Region:** Zuid-Holland **City:** Rotterdam **Latitude:** 51.922501 **Longitude:** 4.479170 **View:** Google Map
duckduckgo.com	ok	**IP:** 40.81.94.43 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ff.search.yahoo.com	ok	**IP:** 98.136.144.138 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
search.yahoo.com	ok	**IP:** 98.136.144.138 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
freegeoip.app	ok	**IP:** 104.21.19.200 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.qwant.com	ok	**IP:** 194.187.168.106 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.199.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
source.android.com	ok	**IP:** 142.250.182.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.openweathermap.org	ok	**IP:** 178.128.25.248 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
raw.githubusercontent.com	ok	**IP:** 185.199.109.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
ac.ecosia.org	ok	**IP:** 52.60.139.71 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
m.search.naver.com	ok	**IP:** 223.130.200.195 **Country:** Korea (Republic of) **Region:** Gyeonggi-do **City:** Seongnam **Latitude:** 37.438610 **Longitude:** 127.137779 **View:** Google Map
ac.search.naver.com	ok	**IP:** 223.130.200.116 **Country:** Korea (Republic of) **Region:** Gyeonggi-do **City:** Seongnam **Latitude:** 37.438610 **Longitude:** 127.137779 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m.baidu.com	ok	**IP:** 45.113.192.101 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
ac.duckduckgo.com	ok	**IP:** 40.81.94.43 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
www.ecosia.org	ok	**IP:** 104.18.15.27 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.bing.com	ok	**IP:** 204.79.197.200 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
yandex.com	ok	**IP:** 5.255.255.80 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

✉ EMAILS

EMAIL	FILE
dev@jfenn.me	me/jfenn/attribouter/wedges/ContributorsWedge.java

HARDCODED SECRETS

POSSIBLE SECRETS
"default_owm_key" : "17a6438b1d63d5b05f7039e7cb52cde7"
"pref_weather_api_key_title" : "API-nøgle"
"pref_weather_api_key_title" : "API-Schlüssel"

PLAYSTORE INFORMATION

Title: Lawnchair 2

Score: 4.1468925 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Personalization **Play Store URL:** ch.deletescape.lawnchair.plah

Developer Details: David Sn, 8230778477483436132, David Sn ul. Siewna 23A/41 31-231 Kraków Poland, https://lawnchair.app, support@lawnchair.info,

Release Date: Jun 10, 2018 **Privacy Policy:** Privacy link

Description:

Lawnchair 2 introduces powerful new features—from Drawer Categories to integration with Android Recents and contextual data in At a Glance. Key Features — Support for Adaptive Icons. — Flexible Desktop, Dock, and Drawer. — Drawer Categories (Tabs & Folders). — Integration with Android Recents.[1] — Automatic Dark Mode. — Contextual data in At a Glance. — Notification Dots. — Integration with Google Feed and Homefeeder.[2] Get Support — twitter.com/lawnchairapp. — t.me/lccommunity. — reddit.com/r/lawnchairlauncher. 1. Requires QuickSwitch (t.me/QuickstepSwitcherReleases). Works on Android 9. 2. Requires Lawnfeed (lawnchair.app/lawnfeed) and Homefeeder (t.me/homefeeder) respectively. Note: this release doesn’t officially support Android 10. Lawnchair 2 uses the Device Administrator permission to lock the screen when a selected gesture is detected. This is optional and disabled by default.

Report Generated by - MobSF v3.5.1 Beta

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.