MOBSF

ANDROID STATIC ANALYSIS REPORT

app_icon

Nest (5.81.0.8)

File Name:	base.apk
Package Name:	com.nest.android
Scan Date:	Jan. 1, 2026, 6:07 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	23	4	0	1

FILE INFORMATION

File Name: base.apk
Size: 45.83MB
MD5: deaf8ee31f5c9af2c61563b90ef77070
SHA1: 70caae7fc3a44558237cb2eede9839c07942c38e
SHA256: 37a9dad08d4e5f537825d0304e29e1704e61a6a9f142e417544d040f4a0de86f

APP INFORMATION

App Name: Nest
Package Name: com.nest.android
Main Activity: com.obsidian.v4.activity.LoginActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 5.81.0.8

Android Version Code: 5810008

APP COMPONENTS

Activities: 91
Services: 36
Receivers: 20
Providers: 6
Exported Activities: 3
Exported Services: 2
Exported Receivers: 6
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Palo Alto, O=Nest, OU=Engineering, CN=Tony Fadell
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-06-02 20:32:25+00:00
Valid To: 2040-05-26 20:32:25+00:00
Issuer: C=US, ST=California, L=Palo Alto, O=Nest, OU=Engineering, CN=Tony Fadell
Serial Number: 0x30fadefe
Hash Algorithm: sha256
md5: d30ac9089e54f92ef169b4e8b42b8972
sha1: 4487bbcd9da4300a9bed37c763cbbb86f0daded0
sha256: 1533d8bedc9f693bc627cc759b7b4d7f7e7f85715e9c0b6e4ea865611fc72da3
sha512: 380642fba1756d6747a4fd48283c64405a50051594dd0ff2ad89ad3f6cee6fb52ba2383d0f99d5232846aa55108ca3203f1c7370387769210faa7a2379d51c0f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d6f656abb122e0e7b38b1266eb53eab85c129063d5f8326af5b8e831ba81d3ab
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.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.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.nest.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<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.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() 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>r8</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</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes4.dex	FINDINGS: Compiler — DETAILS: r8
classes5.dex	FINDINGS: Compiler — DETAILS: r8
classes6.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8
classes7.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check network operator name check FINDINGS: Compiler — DETAILS: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.obsidian.v4.activity.LoginActivity	Schemes: https://, Hosts: home.nest.com, Paths: /login/invite/accept, /login/invite/accept/merge,
com.nestlabs.android.framework.deeplink.DeepLinkRoutingActivity	Schemes: nestmobile://, https://, Hosts: home.nest.com, Paths: /redirect/android, /nest-aware-hanging-entitlement-setup, Path Prefixes: /camera/, /thermostat/, /lock/, /tag/, /security/,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: com.nest.android://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 13 | 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	Activity (com.obsidian.v4.tv.home.TvHomeActivity) 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.
3	Activity (com.nestlabs.android.framework.deeplink.DeepLinkRoutingActivity) 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.
4	Broadcast Receiver (com.nestlabs.android.notificationdisplay.UpdateNotificationChannelsBroadcastReceiver) 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.
5	Broadcast Receiver (com.obsidian.v4.goose.RegisterGeofencesWithOSBroadcastReceiver) 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
6	Broadcast Receiver (com.obsidian.messagecenter.SecureSunsetNotificationScheduleResetBroadcastReceiver) 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	Content Provider (com.dropcam.android.CameraNotificationImageProvider) is not Protected. [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.
8	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	Activity (net.openid.appauth.RedirectUriReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
10	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.
11	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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	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.
13	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 8 | INFO: 3 | SECURE: 0 | SUPPRESSED: 0

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	a2/a.java b2/e.java b3/a.java c4/l.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/f.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/r.java com/bumptech/glide/load/resource/bitmap/a.java com/bumptech/glide/manager/e.java com/bumptech/glide/request/SingleRequest.java com/nestlabs/coreui/components/ListCellComponent.java e2/h.java f2/d.java h2/h.java h2/i.java i2/e.java i2/j.java l4/b.java n2/d.java n2/m.java o4/b.java q/c.java q/p.java q4/a.java r2/a.java u2/d.java u3/a.java u5/a.java yu/a.java z1/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	bt/a.java bt/b.java c5/b.java com/nest/czcommon/structure/j.java com/nestlabs/android/ble/c.java com/obsidian/v4/data/grpc/g.java com/obsidian/v4/fragment/settings/camera/CameraScheduleCreateScheduleFragment.java com/obsidian/weather/ClearDayView.java com/obsidian/weather/ClearNightView.java com/obsidian/weather/CloudView.java com/obsidian/weather/RainView.java com/obsidian/weather/SwayTranslateView.java com/obsidian/weather/WeatherRandom.java com/obsidian/weather/d.java ct/a.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/k0.java io/grpc/internal/n2.java io/grpc/okhttp/e.java nl/Weave/DeviceManager/WeaveDeviceManager.java os/a.java s9/d.java xi/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nest/thermozilla/b.java com/obsidian/v4/activity/LoginActivity.java com/obsidian/v4/data/AndroidClientInfo.java com/obsidian/v4/data/cz/service/a.java com/obsidian/v4/fragment/settings/account/SettingsAccountLegalAboutFragment.java com/obsidian/v4/goose/b.java com/obsidian/v4/log/WeaveSessionLogBuilder.java com/obsidian/v4/pairing/assistingdevice/AssistingDeviceSurveyorImpl.java com/obsidian/v4/tv/home/about/TvAboutActivity.java com/obsidian/v4/utils/NestAppState.java com/obsidian/v4/utils/s.java com/obsidian/v4/widget/survey/Survey.java la/c.java li/d.java
4	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	m3/b.java
5	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/obsidian/v4/timeline/clip/ClipFileMoveJobIntentService.java com/obsidian/v4/utils/p.java hl/b.java m3/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/nestlabs/weave/security/WeaveSecuritySupport.java com/obsidian/v4/activity/AddProductPairingActivity.java hl/b.java pi/c.java
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/nest/utils/w0.java com/obsidian/v4/appupdate/a.java com/obsidian/v4/data/cz/bucket/Quartz.java com/obsidian/v4/g.java mh/g.java
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	bj/c.java pi/d.java uo/g.java x3/o.java x3/q.java x3/r.java x3/s.java x3/t.java x3/v.java
9	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/nestlabs/weave/security/ApplicationKeySupport.java com/nestlabs/weave/security/HKDF.java t4/a.java w8/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/engine/b.java com/bumptech/glide/load/engine/l.java com/bumptech/glide/load/engine/p.java com/nest/czcommon/bucket/a.java com/nest/czcommon/diamond/b.java com/nest/presenter/b.java com/nestlabs/android/notificationdisplay/CameraNotificationConfig.java com/obsidian/protect/topaz/icfetch/ThreadInterconnectCredentials.java com/obsidian/v4/fragment/settings/user/SettingsUserViewModel.java com/obsidian/v4/twofactorauth/TwoFactorAuthDetails.java d2/c.java i1/d.java io/grpc/internal/b3.java pl/b.java
11	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	com/obsidian/alarms/alarmcard/call/CallEmergencyContactActivity.java com/obsidian/v4/familyaccounts/guests/management/GuestDetailsFragment.java hr/a.java
12	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/obsidian/v4/goose/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/nest/utils/b.java com/nestlabs/coreui/components/TextComponent.java com/obsidian/callcard/CallcardActivity.java com/obsidian/googleassistant/ultraflores/AddGoogleAssistantToFlintstoneFragment.java com/obsidian/googleassistant/ultravox/AddGoogleAssistantToQv2Fragment.java com/obsidian/googleassistant/ultravox/UltravoxGoogleAssistantSettingsFragment.java com/obsidian/v4/activity/GoogleNestTosActivity.java com/obsidian/v4/activity/GoogleTokenFetchFragment.java com/obsidian/v4/activity/HomeActivity.java com/obsidian/v4/activity/LoginActivity.java com/obsidian/v4/activity/login/d.java com/obsidian/v4/f.java com/obsidian/v4/fragment/main/shortcut/AppShortcutRoutingActivity.java com/obsidian/v4/fragment/onboarding/apollo/ApolloRhrParentEnrollmentFragment.java com/obsidian/v4/fragment/settings/account/SettingsCropProfileFragment.java com/obsidian/v4/fragment/settings/structure/ConciergeParentSettingsFragment.java com/obsidian/v4/fragment/settings/user/SettingsUserFragment.java com/obsidian/v4/fragment/settings/user/SettingsUserProtectsFragment.java com/obsidian/v4/gcm/actions/CancelNotificationAndLaunchJobIntentServiceBroadcastReceiver.java com/obsidian/v4/goose/healthcheck/speedbump/GooseHealthDownMessageFragment.java com/obsidian/v4/utils/customtabs/CustomTabsHelper.java com/obsidian/v4/utils/f0.java com/obsidian/v4/utils/s.java dn/l.java kg/a.java kg/b.java lf/b.java lf/c.java net/openid/appauth/AuthorizationManagementActivity.java net/openid/appauth/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
			wu/d.java zp/a.java com/nest/utils/b.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/obsidian/googleassistant/ultraflores/AddGoogleAssistantToFlintstoneFragment.java com/obsidian/googleassistant/ultravox/AddGoogleAssistantToQv2Fragment.java com/obsidian/googleassistant/ultravox/UltravoxGoogleAssistantSettingsFragment.java com/obsidian/v4/activity/HomeActivity.java com/obsidian/v4/activity/LoginActivity.java com/obsidian/v4/gcm/actions/CancelNotificationAndLaunchJobIntentServiceBroadcastReceiver.java com/obsidian/v4/goose/healthcheck/speedbump/GooseHealthDownMessageFragment.java com/obsidian/v4/utils/customtabs/CustomTabsHelper.java dn/l.java kg/b.java lf/b.java net/openid/appauth/AuthorizationManagementActivity.java net/openid/appauth/i.java zp/a.java
00058	Connect to the specific WIFI network	wifi control	com/nest/wificommon/Wifi.java
00130	Get the current WIFI information	wifi collection	com/nest/wificommon/Wifi.java hf/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a2/a.java a2/b.java c8/g.java com/obsidian/v4/data/cz/service/BaseAvatarUploadService.java com/obsidian/v4/data/cz/service/GuestAvatarUploadService.java com/obsidian/v4/data/cz/service/InviteeAvatarUploadService.java com/obsidian/v4/data/cz/service/UserAvatarUploadService.java com/obsidian/v4/timeline/clip/ClipFileMoveJobIntentService.java g8/e.java k2/f.java pi/c.java t1/a.java t1/b.java y1/d.java
00089	Connect to a URL and receive input stream from the server	command network	com/obsidian/v4/data/cz/service/BaseAvatarUploadService.java e2/h.java ma/b.java t1/b.java y1/g.java
00030	Connect to the remote server through the given URL	network	e2/h.java t1/b.java
00109	Connect to a URL and get the response code	network command	b4/b.java com/obsidian/v4/data/cz/service/BaseAvatarUploadService.java e2/h.java i4/c.java ma/b.java t1/b.java y1/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/nestlabs/android/location/r.java com/obsidian/v4/data/cz/service/weather/WeatherService.java f8/a.java ma/b.java
00022	Open a file from given absolute path of the file	file	c8/g.java com/nestlabs/weave/security/WeaveSecuritySupport.java com/obsidian/v4/fragment/settings/account/SettingsCropProfileFragment.java com/obsidian/v4/timeline/clip/ClipFileMoveJobIntentService.java hl/b.java pi/a.java pi/c.java t1/a.java t1/b.java uo/g.java w0/a.java y1/d.java
00012	Read data and put it into a buffer stream	file	y1/d.java
00112	Get the date of the calendar event	collection calendar	com/nest/utils/DateTimeUtilities.java com/obsidian/v4/data/cz/service/threads/HistoryServiceThread.java com/obsidian/v4/familyaccounts/guests/scheduling/weekly/a.java
00016	Get location info of the device and put it to JSON object	location collection	com/obsidian/v4/data/cz/service/a.java
00096	Connect to a URL and set request method	command network	com/obsidian/v4/data/cz/service/BaseAvatarUploadService.java ma/b.java t1/b.java y1/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00153	Send binary data over HTTP	http	com/obsidian/v4/data/cz/service/BaseAvatarUploadService.java y1/g.java
00036	Get resource file from res/raw directory	reflection	com/nest/utils/b.java com/obsidian/v4/activity/GoogleTokenFetchFragment.java com/obsidian/v4/f.java com/obsidian/v4/goose/healthcheck/speedbump/GooseHealthDownMessageFragment.java com/obsidian/v4/utils/s.java
00034	Query the current data network type	collection network	com/obsidian/v4/utils/t.java
00162	Create InetSocketAddress object and connecting to it	socket	rr/e.java
00163	Create new Socket and connecting to it	socket	rr/e.java
00091	Retrieve data from broadcast	collection	com/nest/utils/b.java com/obsidian/v4/activity/HomeActivity.java com/obsidian/v4/activity/LoginActivity.java com/obsidian/v4/fragment/main/shortcut/AppShortcutRoutingActivity.java com/obsidian/v4/gcm/FcmRegistrationService.java com/obsidian/v4/utils/Traversal.java net/openid/appauth/AuthorizationManagementActivity.java
00121	Create a directory	file command	com/obsidian/v4/timeline/clip/ClipFragment.java
00125	Check if the given file path exist	file	com/obsidian/v4/timeline/clip/ClipFragment.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	f2/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	c8/g.java
00005	Get absolute path of file and put it to JSON object	file	c8/g.java
00078	Get the network operator name	collection telephony	com/obsidian/v4/log/WeaveSessionLogBuilder.java
00202	Make a phone call	control	com/nest/utils/b.java zp/a.java
00203	Put a phone number into an intent	control	com/nest/utils/b.java zp/a.java
00015	Put buffer stream (data) to JSON object	file	ma/b.java
00108	Read the input stream from given URL	network command	ma/b.java
00192	Get messages in the SMS inbox	sms	com/obsidian/v4/utils/p.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	c3/a.java g9/a.java
00079	Hide the current app's icon	evasion	j1/m.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://nest-mobile-prod.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/733249279899/namespaces/firebase:fetch?key=AIzaSyBm-SGckFe_uBK7Vauuadoo2S-MgNYWsYw is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'block_pairing_legacy_thermostats': 'true', 'camera_timeline_dropstale_limit_surpass_enabled': 'true', 'feature_2fa_upsell_enabled': 'true', 'feature_2fa_upsell_timeout_seconds': '604800', 'feature_app_review_nag_enabled': 'true', 'feature_app_review_nag_max_prompts_allowed': '8', 'feature_app_review_nag_should_show_rating_alert': 'true', 'feature_concierge_subscription_ending_warning_enabled': 'true', 'feature_firebase_vision_qr_scanning_enabled': 'true', 'feature_foundation_camera_port_fallback_enabled': 'true', 'feature_foundation_camera_url_session_streaming_enabled': 'true', 'feature_goose_history_enabled': 'true', 'feature_griffin_account_restrictions_enabled': 'true', 'feature_legacy_nest_aware_eos': 'true', 'feature_mode_switcher_halo_text_enabled': 'true', 'feature_np_gha': '', 'feature_np_gha_ic_fetch': 'true', 'feature_np_gha_protect_notification_settings': 'false', 'feature_nr_enhancements': 'true', 'feature_olive_account_creation_strategy': 'enable_account_creation_gaia_only', 'feature_olive_family_member_invite_discovery_enabled': 'true', 'feature_olive_gaia_account_linking': 'true', 'feature_olive_migration_speedbump_enabled': 'false', 'feature_olive_migration_speedbump_for_non_wwn_users_enabled': 'true', 'feature_olive_migration_speedbump_for_wwn_users_enabled': 'false', 'feature_olive_network_request_timeout_in_millis': '65000', 'feature_olive_nevis_reassignment_speedbump_enabled': 'false', 'feature_olive_token_refresh_delay_before_expiration_in_minutes': '10', 'feature_onboarding_doorbell_theme': 'winter_2025', 'feature_package_detection_enabled': 'true', 'feature_project_hawk_enabled': 'true', 'feature_recaptcha_enabled': 'true', 'feature_rhr_enhancements': 'true', 'feature_rosequartz_docked_callscreen_autolaunch_enabled': 'true', 'feature_seek_to_beginning_of_pill_enabled': 'true', 'feature_show_ultraflores_update_screen_enabled': 'true', 'feature_ultraflores_deeplink_version': '2', 'feature_ultravox_deeplink_version': '2', 'ftr_c_cookie_enabled': 'false', 'min_app_version_force': '', 'min_app_version_warn': ''}, 'state': 'UPDATE', 'templateVersion': '86'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/25	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.READ_CONTACTS, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.GET_ACCOUNTS, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	7/44	android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.c2dm.permission.RECEIVE

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
nexusapi.camera.home.nest.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
one.google.com	ok	**IP:** 172.217.2.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
policies.google.com	ok	**IP:** 142.251.34.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ft.nest.com	ok	**IP:** 35.244.148.22 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
webapi.camera.home.qa.nestlabs.com	ok	**IP:** 35.201.110.95 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 104.18.26.120 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
search.app.goo.gl	ok	**IP:** 192.178.50.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
addressvalidation.googleapis.com	ok	**IP:** 142.251.35.106 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
webapi.camera.home.nest.com	ok	**IP:** 35.201.70.64 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
webapi.camera.home.integration.nestlabs.com	ok	**IP:** 35.227.241.146 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
clients3.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
g.co	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nest.com	ok	**IP:** 35.241.20.76 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
yalehome.com	ok	**IP:** 52.16.8.119 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.googlenestcommunity.com	ok	**IP:** 13.35.196.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
s.www-staging2.dropcam.com	ok	**IP:** 35.190.26.243 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
nest-mobile-prod.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
maps.googleapis.com	ok	**IP:** 142.251.34.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dlp.googleapis.com	ok	**IP:** 172.217.15.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
webapi.camera.home.ft.nest.com	ok	**IP:** 35.241.54.132 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
google.com	ok	**IP:** 192.178.50.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	**IP:** 142.251.35.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
myaccount.google.com	ok	**IP:** 74.125.196.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
nexusapi.camera.home.ft.nest.com	ok	No Geolocation information available.
nexusapi.camera.home.integration.nestlabs.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 172.217.2.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.youtube.com	ok	**IP:** 172.217.165.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.qa.nestlabs.com	ok	**IP:** 35.227.229.96 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
home.nest.com	ok	**IP:** 34.117.101.60 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
home.google.com	ok	**IP:** 142.250.64.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.217.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nexusapi.camera.home.qa.nestlabs.com	ok	No Geolocation information available.
www.handy.com	ok	**IP:** 54.158.190.24 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
play.google.com	ok	**IP:** 172.217.165.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.integration.nestlabs.com	ok	**IP:** 35.227.226.34 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
one-staging.sandbox.google.com	ok	**IP:** 173.194.215.81 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
clients.nest.com	ok	No Geolocation information available.
www.googleapis.com	ok	**IP:** 142.250.64.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
nestrenew.google.com	ok	**IP:** 142.250.64.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.geonames.org	ok	**IP:** 188.40.33.19 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
accounts.google.com	ok	**IP:** 142.251.107.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
store.google.com	ok	**IP:** 142.250.217.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Display		https://reports.exodus-privacy.eu.org/trackers/188

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"address_validation_api_key" : "AIzaSyDelmtWtkHJvFu0l8WXfEoC-hK3bTGUkhw"
"com.google.firebase.crashlytics.mapping_file_id" : "ba2ba9580cdf4573bde45caf8bd12804"
"dev_protect_fetch_credential_enqueue" : "Enqueue"
"dev_protect_fetch_credential_fetch" : "Fetch"
"dev_protect_fetch_credential_upload" : "Upload"
"firebase_database_url" : "https://nest-mobile-prod.firebaseio.com"
"google_api_key" : "AIzaSyBm-SGckFe_uBK7Vauuadoo2S-MgNYWsYw"
"google_crash_reporting_api_key" : "AIzaSyBm-SGckFe_uBK7Vauuadoo2S-MgNYWsYw"

POSSIBLE SECRETS
"maldives_securezilla_alarm_reason_pinna_open_door_bypass" : "Opened"
"maldives_securezilla_alarm_reason_pinna_open_window_bypass" : "Opened"
"maps_api_key" : "AIzaSyBX5oDgQ2QIjSGsqsunNXmeZ0tm9lo4jKA"
"mfa_settings_account_two_step_verification_password" : "Password:"
"nest_capability_auth" : "nest_authentication"
"pairing_agate_intro_video_youtube_key" : "1G4XDW9YG94"
"pairing_rq_install_video_youtube_key" : "TwPS46AZy2o"
"setting_account_pincodes_password" : "Password:"
"settings_session_client_by_company_title" : "%1$s"
C3536F27-7438-4E2D-B59D-D87A5688837F
C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83
7606123e-4282-4ed4-aca1-2374de7fdb61
Y29tLmdvb2dsZS5hbmRyb2lkLmFwcHMuZHJlYW1saW5lci5wcm92aWRlcg==
scysy0lse8KP0mxB1m3cJUZVSt6yqJdEfwkImyE6AIgfrfraw7lJTFU9o04BlPEVmDh

POSSIBLE SECRETS
90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
Ky8PRZkmDkVFZrD3AsSmgEKBgi8rsKPARIHCCwSA29wYRphEl8IBBJb6oqo9ARVCAMaEGNvbS5uZXN0LmFuZHJvaWQiGG5lc3QtaG9tZS1hc3Npc3RhbnQtcHJvZCoPbmVzdF90aGVybW9zdGF0MhJuZXN0LnVsdHJhdm94LnByb2Q4ASIkCiJodHRwOi8vYXNzaXN0YW50Lmdvb2dsZS5jb20vZGV2aWNl
EWDEqkZeEwD6e8QIgI3YbmXzEPhm5keucbcviAwuntf43YAG1jD1FkPBVGYsSrAEKBgi8rsKPARIHCC4SA29wYRpzEnEIBBJt6oqo9ARnCAMaEGNvbS5uZXN0LmFuZHJvaWQiGG5lc3QtaG9tZS1hc3Npc3RhbnQtcHJvZCoPbmVzdF90aGVybW9zdGF0MhVuZXN0LnVsdHJhZmxvcmVzLnByb2Q4AVoNbmVzdG1vYmlsZTovLyIkCiJodHRwOi8vYXNzaXN0YW50Lmdvb2dsZS5jb20vZGV2aWNl
n5wIgdCiOqIZsGyqULdKQn5cQKKMkkX9T3
0fde7f14-864a-4f7f-8dbe-7ac1f4ea4b91
470fa2b4ae81cd56ecbcda9735803434cec591fa
ae2044fb577e65ee8bb576ca48a2f06e
CksBDb3mGzBEAiAaPELPfHOd6ZxNLMTAGAZ0U3115jlq2Jvk45ZPqw
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
CksBDb3mGzBEAiB6RBTRUVoBAlWzTqd2K5dClRklFRUre3q3C2JNKRTkxAIgGjhb9aUAxJsAsZB
PLAdP2gzuu3qQZxRfrfbakI5LovNmWJnre
rhdoHKigrbSwisVrPLIaISrAEKBgjM3bSPARIHCAESA29wYRpzEnEIBBJt6oqo9ARnCAMaEGNvbS5uZXN0LmFuZHJvaWQiGG5lc3QtaG9tZS1hc3Npc3RhbnQtcHJvZCoPbmVzdF90aGVybW9zdGF0MhVuZXN0LnVsdHJhZmxvcmVzLnByb2Q4AVoNbmVzdG1vYmlsZTovLyIkCiJodHRwOi8vYXNzaXN0YW50Lmdvb2dsZS5jb20vZGV2aWNl

POSSIBLE SECRETS
A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085
JTNHuXF347LfUSmgEKBgjM3bSPARIHCAESA29wYRphEl8IBBJb6oqo9ARVCAMaEGNvbS5uZXN0LmFuZHJvaWQiGG5lc3QtaG9tZS1hc3Npc3RhbnQtcHJvZCoPbmVzdF90aGVybW9zdGF0MhJuZXN0LnVsdHJhdm94LnByb2Q4ASIkCiJodHRwOi8vYXNzaXN0YW50Lmdvb2dsZS5jb20vZGV2aWNl
CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D
0123456789ABCDEFGHJKLMNPRSTUVWXY
90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73
5181942b9ebc31ce68dacb56c16fd79f
18ee2ef5-263d-4559-959f-4f9c429f9d11
5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B
d2d3f8ef-9c99-4d9c-a2b3-91c85d44326c
9760508f15230bccb292b982a2eb840bf0581cf5

PLAYSTORE INFORMATION

Title: Nest

Score: 3.8384342 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** com.nest.android

Developer Details: Nest Labs Inc., Nest+Labs+Inc., None, https://nest.com/, support@nest.com,

Release Date: Jun 17, 2015 **Privacy Policy:** Privacy link

Description:

At Google Nest, we make products that are beautiful, helpful and easy to use. The Nest app is no exception. Control your Nest thermostat, arm and disarm your Nest Secure alarm system, see your home with Nest Cam, and get an alert if Nest Protect goes off – all in one place. And receive notifications on your Android phone or tablet. Nest uses sensors, algorithms, and the location of your phone to do the right thing automatically, turning off the heat and turning on the camera when you leave. Forget to set the alarm? It will notice, and send you a Remind Me alert. Nest Learning Thermostat and Nest Thermostat E Thermostats that program themselves to help you save energy. - Change the temperature from the subway or the sofa using your phone. - See how much energy you used, and why. - View and edit your schedule. - Get extreme temperature alerts before your home gets too cold. Nest Secure alarm system - Arm and disarm your home remotely from the app. - Receive a Remind Me alert if you leave home and forget to set the alarm. - Receive a security alert on your phone telling you what triggered the alarm – a door or window opening, or someone entering a room. Nest Protect The smoke and carbon monoxide alarm that thinks, speaks, and alerts your phone. - Get an alert if Nest Protect senses smoke or carbon monoxide. (Requires Wi-Fi and a working internet connection.) - Silence an alarm from your phone with App Silence. (Nest Protect 2nd gen only.) - See the status of your batteries, sensors, and Wi-Fi connection. - Run a Safety Checkup to test all your alarms at once. (Nest Protect 2nd gen only.) - See your Safety History so you know when alerts happened and why. Nest Cam IQ Indoor and Outdoor, Nest Cam Indoor, Nest Cam Outdoor, and Dropcam The security cameras that let you see your home on your phone, inside and out. - Get alerts when there’s activity, and talk back to get someone’s attention. - See what you missed with snapshots of the last three hours. - Check in 24/7 with crisp 1080p HD video (Nest Cam and Dropcam Pro only). - Get person alerts (or familiar face alerts with Nest Cam IQ) and up to 30 days of video history when you subscribe to Nest Aware. (Subscription service sold separately.) Nest Hello Know who’s knocking. - 24/7 video streaming means you’ll never miss a moment. - Designed to show you everything at your doorstep – people head to toe, or packages on the ground. - Knows the difference between a person and a thing. - Notifies you about visitors, even if they don’t ring the bell. - HD Talk and Listen lets you have a seamless conversation with someone at your door. - When you can’t answer the door, quick responses let you reply to visitors with prerecorded audio messages. Nest x Yale Lock The lock for a more secure connected home. - Instead of sharing keys, assign passcodes to people you trust in the Nest app. - Get an alert when someone locks or unlocks the door. - With Home/Away Assist and Auto-Lock, your door can lock itself when you leave. Some features require a working internet connection, Wi-Fi, and/or Bluetooth.

SCAN LOGS

Timestamp	Event	Error

2026-01-01 06:07:58	Generating Hashes	OK
2026-01-01 06:07:59	Extracting APK	OK
2026-01-01 06:07:59	Unzipping	OK
2026-01-01 06:07:59	Parsing APK with androguard	OK
2026-01-01 06:07:59	Extracting APK features using aapt/aapt2	OK
2026-01-01 06:07:59	Getting Hardcoded Certificates/Keystores	OK
2026-01-01 06:08:00	Parsing AndroidManifest.xml	OK
2026-01-01 06:08:00	Extracting Manifest Data	OK
2026-01-01 06:08:00	Manifest Analysis Started	OK
2026-01-01 06:08:00	Performing Static Analysis on: Nest (com.nest.android)	OK
2026-01-01 06:08:01	Fetching Details from Play Store: com.nest.android	OK

2026-01-01 06:08:01	Checking for Malware Permissions	OK
2026-01-01 06:08:01	Fetching icon path	OK
2026-01-01 06:08:01	Library Binary Analysis Started	OK
2026-01-01 06:08:01	Reading Code Signing Certificate	OK
2026-01-01 06:08:02	Running APKiD 3.0.0	OK
2026-01-01 06:08:06	Detecting Trackers	OK
2026-01-01 06:08:08	Decompiling APK to Java with JADX	OK
2026-01-01 06:08:34	Converting DEX to Smali	OK
2026-01-01 06:08:34	Code Analysis Started on - java_source	OK
2026-01-01 06:08:36	Android SBOM Analysis Completed	OK
2026-01-01 06:08:41	Android SAST Completed	OK

2026-01-01 06:08:42	Android API Analysis Started	OK
2026-01-01 06:08:43	Android API Analysis Completed	OK
2026-01-01 06:08:43	Android Permission Mapping Started	OK
2026-01-01 06:08:57	Android Permission Mapping Completed	OK
2026-01-01 06:08:57	Android Behaviour Analysis Started	OK
2026-01-01 06:09:00	Android Behaviour Analysis Completed	OK
2026-01-01 06:09:00	Extracting Emails and URLs from Source Code	OK
2026-01-01 06:09:03	Email and URL Extraction Completed	OK
2026-01-01 06:09:03	Extracting String data from APK	OK
2026-01-01 06:09:03	Extracting String data from Code	OK
2026-01-01 06:09:03	Extracting String values and entropies from Code	OK

2026-01-01 06:09:06	Performing Malware check on extracted domains	OK
2026-01-01 06:09:12	Saving to Database	OK

Report Generated by - MobSF v4.4.4

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.