Quokka

Android Application Analysis

InsecureShop

com.insecureshop
1.0
SHA1: 5a68ca276a1003db3677bcd206b1f4b9bc5caa81

Submitted Date: 06/05/2024 - 11:14:06 PM
Submission Method: API - Binary Submission
Analysis Date: 06/05/2024 - 11:14:07 PM
Q-MAST Version: 2.149.0

Threat Score

- Critical Risk
- High Risk
- Medium Risk
- Low Risk

- 1 High
- 8 Medium
- 5 Low

Quokka

Security Findings

- Vulnerable to known OS attacks
- Requested excessive permissions
- Allows backup
- RASP not detected
- No data at rest encryption
- Application programmatically leaks data
- Application does not check for trusted environment
- Does not use secure key or random number generation
- HTTP URLs found in application
- Does not use platform keychain

- App does not contain a known severe vulnerability
- No malware detected
- Uses proper SSL verification
- Does not have admin privileges
- Does not kill other apps
- No privilege escalation detected
- Debuggable not enabled
- Does not download in the background
- No dynamic use of hard coded credentials
- Does not access risk files over the network
- App does not contain a known high-risk vulnerability
- App does not expose files in private container
- App does not enable factory reset attack
- App does not enable arbitrary command execution
- No hard coded credentials
- No Java classes loaded dynamically
- No external library loaded dynamically
- Does not execute native code
- Does not remain persistent in memory
- No incorrect SQL
- Does not contain code with improper SSL verification
- No unencrypted network connections made
- App does not leak logs to public storage
- SSL pinning detected

Privacy Findings

- Accesses contacts

- App does not communicate with high risk locations
- No passwords exposed
- Does not expose sensitive information
- No in app purchases
- No connections to foreign countries
- Stores files properly
- Does not expose low risk sensitive information
- Does not track user behaviour
- No ad network integration
- No cloud storage integration
- No social network integration
- No access to Account Manager
- Does not access subscriber ID
- Does not access unique device ID
- Does not access device SIM number
- Does not access device phone number
- Does not access calendar

Device Functionality Findings

- Writes to the external storage
- Accesses the external storage
- Accesses the Internet

- Does not send SMS/MMS messages
- Does not receive SMS/MMS messages
- Does not read SMS
- Does not record audio
- Does not access camera
- Does not make phone calls
- Does not access Bluetooth
- Does not access NFC
- Does not access location

Quokka

- ✅ App does not contain a known medium-risk vulnerability
- ✅ Does not have leftover files after uninstall
- ✅ App does not contain a known low-risk vulnerability

Additional Evidence

- ⓘ Application Information
- ⓘ Permissions Requested
- ⓘ AV Scan Results
- ⓘ App Protection Analysis
- ⓘ App Transport Security

Quokka
Standard Results

HIGH

Exploitable **Vulnerable to known OS attacks** static **CVSS Score: 8.6** **CWE-284**

The application supports operating system versions that have known vulnerabilities. These vulnerabilities enable attacks on the application which could compromise the user or developer.

Threat Details

An attacker can exploit the application on devices running a vulnerable operating system version. Th is may be used to attack users running the applica tion and/or exploit the application itself.

Regulations

Fail OWASP: M1: Improper Platform Usage
Fail OWASP: M9: Reverse Engineering
Fail OWASP: M8: Code Tampering
Fail GDPR: Article 32: Security of Processing
Fail GDPR: Article 5: Principles Relating to Processing of Personal Data
Fail GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We determine if the application supports operating system versions that have known vulnerabilities. This is d etermined by examining the application manifest for the minimum supported operating system version.

Remediation

The developer should increase the minimum supported operating system version to support versions which do not have known vulnerabilities that enable attacks on the user or application.

Finding Impact

Users of the application may be targeted through the operating system attack vectors. This could expose use r information related to the application and enable attackers to perform actions on behalf of the user. Altern atively, these vulnerabilities could be used to exploit application functions that could compromise or defraud the development organization.

Evidence

Vulnerable OS Version

CVE-2017-13156

An elevation of privilege vulnerability in the Android system which may affect any SDK Version lower than 24

Current Minimum SDK Version Supported: **16**

Requested excessive permissions

hybrid | CVSS Score: 4.4 | CWE-250

MEDIUM

The application has access to more permissions than it likely needs. This is determined by mapping the requested permissions in the AndroidManifest.xml file to the constants and methods seen inside the application.

Threat Details

Extra permissions increase the attack surface on t he device if an application is exploited via another attack vector. Additionally it is a poor developmen t practice to request functionality that is not need ed for execution.

Regulations

- Fail OWASP: M7: Client Code Quality
- Fail OWASP: M10: Extraneous Functionality
- Fail NIAP: FDP_DEC_EXT.1.1
- Fail NIAP: FDP_DEC_EXT.1.2

Test Performed

We scan the application's byte code and packaged SDKs for all of the methods that are called. Based off of th ese findings and a mapping between method calls and required permissions we determine which permission s which were requested by the application, but not needed.

Remediation

The permissions can be reviewed to confirm which ones are needed for the core functionality of the applicati on. Extra permissions can be removed from the AndroidManifest.xml file to remove access.

Finding Impact

Having extra permissions increase the attack surface on the device if an application is exploited via another a ttack vector. Additionally it is a poor development practice to request functionality that is not needed for exec ution. This can decrease trust from the user and add unnecessary bloat to the application.

Evidence

Extra Permissions:

android.permission.READ_CONTACTS
android.permission.WAKE_LOCK

Accesses contacts

hybrid | CVSS Score: 2.3

MEDIUM

The application can access the user's contacts. This functionality is allowed by the permissions android.permission.WRITE_CONTACTS and/or android.permission.READ_CONTACTS.

Threat Details

Access to write user's contacts data should be con sidered dangerous. The application has no restrict ions for the type of contacts it can create and coul d create fake contacts to trick the user or modify e xisting contact details.

Regulations

Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We determine if the application requires the permission(s) to read and or write to the device's contacts.

Remediation

android.permission.READ_CONTACTS and/or android.permission.WRITE_CONTACTS can be removed from the application's AndroidManifest.xml file to remove access.

Finding Impact

Developer should ensure that this permission is needed for the core functionality of the application. Extrane ous permissions and functions increase the size of the application. Additionaly users are wary of overly permi ssive apps.

Evidence

Relevant Permission(s) Requested:
android.permission.READ_CONTACTS

MEDIUM

Exploitable **Allows backup** static CVSS Score: 4.6 CWE-497

The application allows its private files to be backed up from the device. This allows anyone with physical access to the device the ability to extract these files which potentially can contain sensitive data.

Threat Details

The allowBackup option in AndroidManifest.xml m eans the application files will be included when th e user backs up their device. This can be a proble m if any sensitive user or application data is saved or cached on the device.

Regulations

Fail OWASP: M2: Insecure Data Storage
Fail OWASP: M6: Insecure Authorization
Fail OWASP: M9: Reverse Engineering
Fail NIAP: FPT_TUD_EXT.1.3
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Fail GDPR: Article 17: Right to be Forgotten
Fail GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We verify if the application's manifest contains the proper flags to allow backup.

Remediation
The developer should explicitly set the allowBackup option to "false" in the AndroidManifest.xml file.

Finding Impact
Any data stored locally by the application is vulnerable to backup to un-vetted machines or servers. This setti ng should only be used if local file data created by the app is not sensitive.

Evidence
allowBackup set to true in AndroidManifest.xml

MEDIUM

RASP not detected
hybrid | CVSS Score: 3.9 | CWE-919

A RASP library was not detected in the application.

Threat Details
RASP libraries help to secure apps against reverse engineering and other exploits on end user device s. Without RASP the app may be more vulnerable t o these types of attacks.

Regulations
Fail OWASP: M3: Insecure Communication

Test Performed
We check for signatures of known RASP libraries.

Remediation
The developer should incorporate an open source or paid RASP library in their application.

Finding Impact
The backend connections performed by the application may be intercepted, monitored, or changed. This coul d lead to leakage of user data, unexpected application behavior, and exposure of organization sensitive data.

Evidence
The RASP library that was detected can be seen in the App Protection section of the report. If none was detected, this item will be flagged.

MEDIUM

Exploitable Writes to the external storage
hybrid | CVSS Score: 2.3 | CWE-922

The application can write to the external storage on the device. This functionality is allowed by the permission.WRITE_EXTERNAL_STORAGE and this permission implicitly gives access to android.permission.READ_EXTERNAL_STORAGE.

Threat Details

Access to the device's external storage allows the application to view and modify any public files the user has saved, downloaded, or that were created by other applications. Application should be vette d to ensure it can be trusted with access to the us er's downloads directory and various application fi les.

Regulations

Fail OWASP: M2: Insecure Data Storage
Fail OWASP: M7: Client Code Quality
Review NIAP: FDP_DEC_EXT.1.1
Fail NIAP: FMT_CFG_EXT.1.2
Review GDPR: Article 32: Security of Processing
Fail GDPR: Article 5: Principles Relating to Processing of Personal Data
Fail GDPR: Article 17: Right to be Forgotten

Test Performed

We identify if during Dynamic Analysis that the application writes data to the external storage of the device.

Remediation

android.permission.WRITE_EXTERNAL_STORAGE can be removed from the application's AndroidManifest.xml file to remove access.

Finding Impact

Data written to external storage is accessible to any other application or user on the device. Developer shoul d ensure that they need to write data to external storage. If so, data written to the external storage should no t be sensitive or would expose user or organizational data.

Evidence

Relevant Permission(s) Requested:
android.permission.WRITE_EXTERNAL_STORAGE

MEDIUM

No data at rest encryption

hybrid | CVSS Score: 4.0 | CWE-311

The application encrypts data on the device. We monitor for encryption operations during the Dynamic Analysis of the application.

Threat Details

If any sensitive data is handled by the application i t is good practice to encrypt this data when stored locally. If the encryption operations are not seen it may be easier for attackers to exploit the informat ion handled by this app.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M5: Insufficient Cryptography
Review OWASP: M7: Client Code Quality
Review NIAP: FDP_DAR_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data

Test Performed

We check to identify the presence of any encryption being performed on data stored on the file system throu ghout the application's Dynamic Analysis.

Remediation
The developer should use encryption for storing sensitive data.

Finding Impact
Encrypting data at rest should be considered mandatory if the application is storing sensitive data on the device. Without an extra level of encryption the data stored on the device, even in the application's private container, can be exposed if the device is comprimised. If there is no sensitive data stored on the device you likely will not need encryption at rest.

Evidence

Dynamic Method Calls:
None

MEDIUM

Exploitable **Application programmatically leaks data** hybrid **CVSS Score: 5.7**
CWE-200

The application leaks data via software defined paths.

Threat Details
Applications with this vulnerability will programmatically leak data to insecure locations. Users of this application may have sensitive data exposed through this vector.

Regulations
Fail OWASP: M7: Client Code Quality
Fail OWASP: M2: Insecure Data Storage
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data

Test Performed
We evaluate the application bytecode and determine if information gathered from sensitive Android API calls reaches an insecure location (e.g. logs, network, external storage).

Remediation
The developer should review the locations provided in the evidence for this item and modify the logic to prevent the data from reaching the insecure location.

Finding Impact
The user of the application may have significant data exposure because of this vulnerability.

Evidence

Doppler Result - PII Leakage

Violation Type	Location	Risk
PII Leakage	`src/com/insecureshop/LoginActivity.smali`	moderate

MEDIUM

Exploitable **Application does not check for trusted environment** dynamic

CVSS Score: 5.0 CWE-284

The application does not check to ensure the operating environment can be trusted.

Threat Details

Applications that do not check for a trusted operating environment may be vulnerable to reverse engineering and exploitation.

Regulations

Fail OWASP: M9: Reverse Engineering

Test Performed

We monitor for health checks on the operating environment of the application. This includes checks for rooted and jailbroken devices among others.

Remediation

The developer should add checks for the health of the operating environment. There are many open source libaries that provide this functionality and most application protection providers will include these checks as well.

Finding Impact

The developer of the application may have their application exploited to get around the standard application workflows.

Evidence

Kryptowire is monitoring for health checks on the operating environment of the application, this item is flagged if no health checks are found.

LOW

Accesses the external storage hybrid CVSS Score: 3.2

The application can read the external storage on the device. This functionality is allowed by the permission.READ_EXTERNAL_STORAGE.

Threat Details

Access to the device's external storage allows the application to view any public files the user has saved, downloaded, or that were created by other applications. Application should be vetted to ensure it can be trusted with access to the user's downloads directory and various application files.

Regulations

Review NIAP: FDP_DEC_EXT.1.2

Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject

Review GDPR: Article 6: Lawfulness of Processing

Test Performed
We identify if the application requires permission to read external storage on the device.

Remediation
android.permission.READ_EXTERNAL_STORAGE can be removed from the application's AndroidManifest.xml file to remove access. Note that any application that has the related permission android.permission.WRITE_EXTERNAL_STORAGE will be given access to this permission by default and this must be removed from the AndroidManifest.xml as well.

Finding Impact
Developer should ensure that this permission is needed for the core functionality of the application. Extraneous permissions and functions increase the size of the application. Additionaly users are wary of overly permissive apps.

Evidence

Relevant Permission(s) Requested:
android.permission.READ_EXTERNAL_STORAGE

LOW

Accesses the Internet hybrid CVSS Score: null

The application can access open network sockets on the device. This functionality is allowed by the android.permission.INTERNET permission.

Threat Details
Access to the internet should be considered normal for any application that has a backend infrastructure. This should only be considered a risk if the application purports to only save data locally on the device.

Regulations

Test Performed
We identify if the application requires permission to open network sockets for communication.

Remediation
android.permission.INTERNET can be removed from the application's AndroidManifest.xml file to remove access.

Finding Impact
Developers should be aware of all potential network connections in their application. What data is sent and where is very important for not violating privacy regulations like GDPR. Ensure not only developer source code is considered, but also data handled by third-party libraries or frameworks.

Evidence

Relevant Permission(s) Requested:
android.permission.INTERNET

Network Traffic

LOW

Exploitable **Does not use secure key or random number generation** dynamic

CVSS Score: 4.0 **CWE-338**

The application does not utilize javax.crypto.KeyGenerator and/or java.security.SecureRandom to generate secure cryptographic keys or random numbers.

Threat Details

Securely generating cryptographic keys and secure random numbers is essential in secure encryption of data. Using insecure random number or key generation will make it easier for attackers to reverse encryption potentially leading to exposure of the encrypted data.

Regulations

Fail OWASP: M5: Insufficient Cryptography
Fail OWASP: M7: Client Code Quality
Fail NIAP: FCS_RBG_EXT.1.1
Fail GDPR: Article 32: Security of Processing
Fail GDPR: Article 5: Principles Relating to Processing of Personal Data
Fail GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We monitor for usage of javax.crypto.KeyGenerator and java.security.SecureRandom during Dynamic Analysis.

Remediation

The developer should use platform provided methods for securely generating cryptographic keys and secure random numbers. More information on this process can be found here https://developer.android.com/reference/javax/crypto/KeyGenerator.

Finding Impact

Securely generating cryptographic keys and secure random numbers is essential in secure encryption of data. Using insecure random number or key generation will make it easier for attackers to reverse encryption potentially leading to exposure of the encrypted data.

Evidence

Kryptowire captures the interactions with the platform provided APIs for securely generating random numbers and cryptographic keys. No calls to these APIs were observed.

Quokka

HTTP URLs found in application

static | CVSS Score: 3.1 | CWE-5

LOW

The application contains URL(s) that specify the HTTP protocol.

Threat Details

If any sensitive data is exchanged over the network through the application it is essential to use encrypted network communications. If the application does not use encrypted connections the app should not have access to any sensitive functionality or data.

Regulations

Review OWASP: M3: Insecure Communication
Fail OWASP: M7: Client Code Quality
Review NIAP: FTP_DIT_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We scan the application during Static Analysis to find URLs that specify the insecure HTTP protocol (e.g. http://www.example.com)

Remediation

The developer should use encryption for any network connections. This is most often achieved through HTTPS using TLS 1.2 and SSL certificates. More information can be found here, https://developer.android.com/training/articles/security-ssl. Unused HTTP URLs should also be trimmed from the codebase to stay in line with best practices.

Finding Impact

Encrypting data in transit should be considered mandatory if the application is sending sensitive data over the network. Without encryption the data sent over the network can be exposed at any point between the client and the server. This can lead to data leakage and provide a view into the application and/or server operations.

Evidence

Constants Data

Type	Value
URL	http://schemas.android.com/apk/res/android
URL	http://schemas.android.com/apk/res-auto

Type	Value
URL	http://stackoverflow.com/a/4410331

LOW

Does not use platform keychain dynamic CVSS Score: 4.0

The application does not utilize android.security.KeyChain and/or java.security.KeyStore to store trusted certificates and/or keys.

Threat Details

Securely storing trusted certificates and keys is essential in secure authentication. Using insecure certificate or key stores will make it easier for attackers to defeat authentication or expose the trusted credentials.

Regulations

Fail OWASP: M4: Insecure Authentication
Fail NIAP: FCS_STO_EXT.1.1

Test Performed

We monitor for usage of android.security.KeyChain and java.security.KeyStore during Dynamic Analysis.

Remediation

The developer should use platform provided methods for securely storing trusted certificates and keys. More information on this process can be found here https://developer.android.com/reference/android/security/KeyChain.

Finding Impact

Securely storing trusted certificates and keys is essential in secure authentication. Using insecure certificate or key stores will make it easier for attackers to defeat authentication or expose the trusted credentials. This could lead to user or organizational data loss and unauthorized access to data.

Evidence

Not Available

PASSED

Exploitable App does not communicate with high risk locations dynamic

CVSS Score: 9.1 CWE-668

Threat Details

Network requests were observed that terminated in a known high risk location. Locations are deemed high risk when there are sanctions defined for organizations operating in them. Data sent to and received in these network requests should be considered compromised due to the lack of protections and enforcement on organizations operating in these locations.

Regulations

Review OWASP: M3: Insecure Communication

Test Performed

We examine all network traffic to determine the countries that the application connects to.

PASSED

Exploitable **App does not contain a known severe vulnerability** hybrid

CVSS Score: 9.5 CWE-829

Threat Details

A vulnerability was identified in a library packaged in the application. The severity and identifier of the specific vulnerability can be seen below.

Regulations

Review OWASP: M8: Code Tampering

Review OWASP: M9: Reverse Engineering

Test Performed

The application binary is processed through a dedicated library and SDK parsing engine which identifies the included libraries and SDKs by their code signatures. The engine also identifies the version of the artifact. This information is used to query for known CVEs associated with the library or SDK name and version. Full results are available in Kryptowire's Software-Bill-of-Materials (SBOM) report in the Kryptowire MAST Portal UI.

PASSED

Exploitable **No malware detected** static CVSS Score: 9.3 CWE-506

Threat Details

This application should not be installed on any device for any reason. Malware is present in the app.

Regulations

Review OWASP: M6: Insecure Authorization

Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We run the application and any embedded files such as PDFs through a series of anti-virus engines to identify any known malware.

PASSED

Exploitable **Uses proper SSL verification** dynamic CVSS Score: 10.0 CWE-295

Threat Details

Communications over the network are insecure. A ny sensitive data transmitted to or from this applic ation could be intercepted, altered, or stolen.

Regulations

Review OWASP: M3: Insecure Communication
Review OWASP: M7: Client Code Quality
Review NIAP: FCS_TLSC_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

Scans were performed on the application's byte code and any packaged SDKs to search for custom SSL mana gers that bypass proper SSL verification. These custom implementations should perform checks on the given certificate to determine if it is valid or not. The identified class returns no errors which therefore accept all SS L certificates. More information can be found here

PASSED

Does not send SMS/MMS messages hybrid CVSS Score: 2.3

Threat Details

Access to send SMS messages should be consider ed dangerous. The application can send content o f the apps choosing to any SMS enabled number. This could be used for fraudulent communication and paid SMS services.

Regulations

Review NIAP: FDP_DEC_EXT.1.2

Test Performed

We identify through Dynamic Analysis if the application sends an SMS/MMS message during execution.

PASSED

Does not receive SMS/MMS messages

hybrid | CVSS Score: 2.3

Threat Details

Access to receive the user's SMS messages should be considered dangerous. There is no restriction f or the SMS threads the app has access to enabling the application to get the full text of every SMS me ssage received on the device.

Regulations

Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We identify if the application requires permission to intercept SMS/MMS messages.

PASSED

Exploitable Does not have admin privileges

static | CVSS Score: 7.7 | CWE-250

Threat Details

Device administrator access should only be allowe d on trusted applications used to manage the depl oyment of mobile devices in an organization. This permission should not be given to any third-party or in-house application for any other reason.

Regulations

Review OWASP: M6: Insecure Authorization
Review NIAP: FDP_DEC_EXT.1.1
Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We test to see if the application requests the ACCESS_SUPERUSER permission in it's Manifest or if we observe an intent sent with a parameter of android.app.action.ADD_DEVICE_ADMIN during dynamic analysis.

PASSED

Does not kill other apps

static | CVSS Score: 3.8 | CWE-250

Threat Details

The application can use this permission to kill bac kground processes of other applications on the de vice. This could be used as a denial of service agai nst other installed applications.

Regulations

Review OWASP: M6: Insecure Authorization
Review OWASP: M7: Client Code Quality
Review NIAP: FDP_DEC_EXT.1.1

Test Performed

We determine if the application declares the need for the KILL_BACKGROUND_PROCESSES permission in it's Manifest.

PASSED

Exploitable **No privilege escalation detected** dynamic CVSS Score: 7.7 CWE-648

Threat Details

Root access allows the application to gain full cont rol of a rooted device. Applications do not need ro ot access for any legitimate functions and should not be installed if they attempt to access it.

Regulations

Review OWASP: M7: Client Code Quality
Review OWASP: M6: Insecure Authorization

Test Performed

We identify an attempt by the application during Dynamic Analysis to gain root access on the device. This is a chieved by the application issuing the appropriate command line command during it's execution.

PASSED

Exploitable **No passwords exposed** dynamic CVSS Score: 6.5 CWE-522

Threat Details

Exposed passwords can be used to access secure accounts of the application and/or network serve r. If the password is re-used across other sensitive accounts an attacker could access additional sensi tive functionality and data.

Regulations

Review OWASP: M4: Insecure Authentication
Review OWASP: M7: Client Code Quality
Review NIAP: FPR_ANO_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We monitor all network traffic and file access generated by the application during Dynamic Analysis for user passwords being leaked.

PASSED

Exploitable **Does not expose sensitive information** dynamic CVSS Score: 5.3

CWE-200

Threat Details

Sensitive information should be carefully reviewed to ensure it is only shared when absolutely necessary. Kryptowire highlights ALL sensitive information sent, including those to Google, & the app developer to ensure the user is aware of all connections. Sharing of device metadata and unique user IDs (advertising IDs, generic user identifiers, etc) can be used in conjunction with other collected data to track users and identify them based off what seems to be innocuous information.

Regulations

Review OWASP: M7: Client Code Quality

Review NIAP: FPR_ANO_EXT.1.1

Review GDPR: Article 44 - General Principle for Transfers to Third Countries or International Organizations

Test Performed

We scan all network traffic generated during Dynamic Analysis for any sensitive information. This includes both plain text HTTP and encrypted HTTPS.

PASSED

Exploitable **Debuggable not enabled** static CVSS Score: 8.4 CWE-489

Threat Details

Debugging functionality gives access to application logs and other privileged details. This can expose sensitive information and allow for insight on an application's internal functions.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M6: Insecure Authorization
Review OWASP: M7: Client Code Quality
Review OWASP: M9: Reverse Engineering
Review NIAP: FPT_TUD_EXT.1.3
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We verify if the "debuggable" flag is set in the application's manifest or not.

PASSED

Does not download in the background

static CVSS Score: 5.1 CWE-494

Threat Details

Unknown and potentially unsafe files can be save d on the user's device without their knowledge.

Regulations

Review NIAP: FDP_DEC_EXT.1.1

Test Performed

We test to see if the application requests the DOWNLOAD_WITHOUT_NOTIFICATION permission in it's Manife st. This permission allows the application to hide UI notifications for when a file is downloaded.

PASSED

Exploitable No dynamic use of hard coded credentials

dynamic CVSS Score: 6.5 CWE-798

Threat Details

Data encrypted or decrypted with hard-coded cry ptographic keys is vulnerable to exposure. Attacke rs could gain access to the key(s) by extracting the m from the application.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M5: Insufficient Cryptography
Review OWASP: M7: Client Code Quality
Review NIAP: FMT_CFG_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

Scans were performed on the application's byte code and any packaged SDKs to search for hard-coded credentials used in cryptographic functions. These codes are declared as constant values within the application's code. The cryptographic keys were observed at runtime during dynamic analysis.

PASSED

Does not access risk files over the network

dynamic | CVSS Score: 6.3 | CWE-829

Threat Details

Accessing compressed files, executable files, and other code related file types may introduce different functionality to an application than the functionality that was approved by the application marketplace. Additionally, if the developer does not correctly validate the signature of the accessed file an attacker may alter its contents.

Regulations

Review OWASP: M10: Extraneous Functionality
Review OWASP: M8: Code Tampering

Test Performed

We monitor the network communications during dynamic analysis for file types that may be considered risky. These include compressed files, executable files, and other code related file types.

PASSED

Exploitable App does not contain a known high-risk vulnerability

hybrid | CVSS Score: 7.9 | CWE-829

Threat Details

A vulnerability was identified in a library packaged in the application. The severity and identifier of th e specific vulnerability can be seen below.

Regulations

Review OWASP: M8: Code Tampering
Review OWASP: M9: Reverse Engineering

Test Performed

The application binary is processed through a dedicated library and SDK parsing engine which identifies the i ncluded libraries and SDKs by their code signatures. The engine also identifies the version of the artifact. This information is used to query for known CVEs associated with the library or SDK name and version. Full results are available in Kryptowire's Software-Bill-of-Materials (SBOM) report in the Kryptowire MAST Portal UI.

PASSED

Exploitable **App does not expose files in private container** hybrid CVSS Score: 6.6

CWE-311

Threat Details

Files in the applications private container may con tain sensitive user or application data. If they are s et to world accessible any application or user on t he device may access them.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M9: Reverse Engineering
Review NIAP: FMT_CFG_EXT.1.2

Test Performed

We run a permission check on the files in the applications private container to see if they are world-accessible (either read, write, or execute).

PASSED

Exploitable **App does not enable factory reset attack** hybrid CVSS Score: 9.3

CWE-306

Threat Details

Applications with this vulnerability are a serious th reat to the user of the device. Programmatic factor y reset allows attackers to completely wipe all data on the device without user permission which coul d lead to significant data loss and/or denial of serv ice.

Regulations

Review OWASP: M7: Client Code Quality
Review OWASP: M8: Code Tampering
Review OWASP: M6: Insecure Authorization

Test Performed

We evaluate the interfaces in the application and determine if there is a path for attackers to exploit them lea ding to factory reset the device.

PASSED

Exploitable **App does not enable arbitrary command execution** hybrid

CVSS Score: 9.6 CWE-77

Threat Details

Applications with this vulnerability are a serious th reat to the user of the device. Command executio n allows attackers to perform arbitrary commands on the system which can lead to exposure of data, denial of service, and compromise of the applicati on or device.

Regulations

Review OWASP: M7: Client Code Quality
Review OWASP: M8: Code Tampering
Review OWASP: M6: Insecure Authorization

Test Performed

We evaluate the interfaces in the application and determine if there is a path for attackers to exploit them lea ding to arbitrary command execution on the device.

PASSED

No hard coded credentials static CVSS Score: 6.2 CWE-798

Threat Details

Data encrypted or decrypted with hard-coded cry ptographic keys is vulnerable to exposure. Attacke rs could gain access to the key(s) by extracting the m from the application.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M5: Insufficient Cryptography
Review OWASP: M7: Client Code Quality
Review NIAP: FMT_CFG_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

Scans were performed on the application's byte code and any packaged SDKs to search for hard-coded credentials used in cryptographic functions. These codes are declared as constant values within the application's code.

PASSED

No Java classes loaded dynamically

dynamic | CVSS Score: 4.5 | CWE-470

Threat Details

If the developer does not verify the security and validity of the dynamically loaded code it is possible it could introduce vulnerabilities, flaws, or unintended functionality in the application.

Regulations

Review OWASP: M6: Insecure Authorization
Review NIAP: FPT_API_EXT.1.1
Review GDPR: Article 17: Right to be Forgotten

Test Performed

We monitored the application during runtime to see if it loads any Java classes through the methods provided in the Android API.

PASSED

No in app purchases

static | CVSS Score: 2.0

Threat Details

Purchases can be made with the user's Google account. In-app purchases can be used to trick users into payments for superfluous reasons.

Regulations

Review NIAP: FDP_DEC_EXT.1.1

Test Performed

We determine if the application requires the com.android.vending.BILLING permission in it's Manifest.

PASSED

Does not read SMS

hybrid | CVSS Score: 2.3

Threat Details

Access to read the user's SMS messages should be considered dangerous. There is no restriction for t he SMS threads the app has access to enabling th e application to get the full text of every SMS mess age on the device.

Regulations

Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We identify if the application requires permissions that provide access to reading the device's SMS messages.

PASSED

No external library loaded dynamically

dynamic | CVSS Score: 3.9 | CWE-470

Threat Details

If the developer does not verify the security and v alidity of the dynamically loaded library it is possib le it could introduce vulnerabilities, flaws, or unint ended functionality in the application.

Regulations

Review OWASP: M6: Insecure Authorization
Review NIAP: FPT_API_EXT.1.1
Review GDPR: Article 17: Right to be Forgotten

Test Performed

All execution during Dynamic Analysis is monitored for the loading of an external library. More information ca n be found here

PASSED

Does not execute native code

dynamic | CVSS Score: 3.6

Threat Details

Running native code indicates usage of non-platfo rm provided APIs or libraries. These libraries may be less secure or stable.

Regulations

Review OWASP: M6: Insecure Authorization
Review NIAP: FPT_API_EXT.1.1
Review GDPR: Article 17: Right to be Forgotten

Test Performed

We identify any execution of calls to native code throughout the Dynamic Analysis process. More information can be found here

Does not record audio

hybrid | CVSS Score: 2.3

PASSED

Threat Details

Access to record audio on the device should be co nsidered dangerous. The application has the adde d capability to record audio in the background pri or to Android 9.

Regulations

Review NIAP: FDP_DEC_EXT.1.1

Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject

Review GDPR: Article 6: Lawfulness of Processing

Test Performed

Through the Dynamic Analysis of the application we identify if the application records audio from the device's microphone.

Does not access camera

hybrid | CVSS Score: 2.3

PASSED

Threat Details

Access to the camera on a device allows an applica tion to take pictures, record video, and view a live output of the camera view. Applications should be reviewed carefully to determine if they need acces s to these features to support their core functional ity. Application developer and country of origin sh ould also be taken into account when reviewing if the application should be run with this access.

Regulations

Review NIAP: FDP_DEC_EXT.1.1

Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject

Review GDPR: Article 6: Lawfulness of Processing

Test Performed

Through the Dynamic Analysis of the application we identify if the application accesses the camera to record audio or take pictures.

No connections to foreign countries

dynamic | CVSS Score: 4.3

PASSED

Threat Details

Connections to other countries can be important for many regulations and application standards, one prominent example is GDPR in the EU. Evaluators should consider what level of access and information the app has and look at which countries are connected to in order to determine the threat profile.

Regulations

Review GDPR: Article 44 - General Principle for Transfers to Third Countries or International Organizations

Test Performed

We examine all network traffic to determine the countries that the application connects to.

Does not remain persistent in memory

static | CVSS Score: 3.8 | CWE-250

PASSED

Threat Details

An application that remains persistent in the background can put an unnecessary drain on the device's battery. This can be happen from a large amount of processing or network calls that are performed by the application even when it's in background. The permission is also deprecated as of API level 15 and may not be supported on modern versions of the Android OS.

Regulations

Review OWASP: M7: Client Code Quality

Review NIAP: FDP_DEC_EXT.1.1

Test Performed

We determine if the application declares the need for the PERSISTENT_ACTIVITY permission in it's Manifest.

Exploitable No incorrect SQL

dynamic | CVSS Score: 4.1 | CWE-89

PASSED

Threat Details

SQL injection allows for attackers to modify the int ended query to the database. Typical attacks inclu de truncating the intended query and adding a sec ondary query to pull, taint, or modify data that is u sually inaccessible. These type of attacks can expo se sensitive data, change the behavior of the app, allow for easier reverse engineering, and more.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M7: Client Code Quality
Review NIAP: FMT_CFG_EXT.1.2
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data

Test Performed

We check to see if the application makes an insecure SQL query by provided a raw string to the query. This do es not apply to CREATE or PRAGMA queries since it is standard to issue raw string queries for those operation s.

PASSED

Exploitable **Stores files properly** hybrid CVSS Score: 4.4 CWE-313

Threat Details

Any data stored in files saved with these flags can be read or written by other applications or users o n the device without special privileges. If sensitive data is stored in these files it is exposed to any oth er software running on the device and is not prote cted by the default privacy provided by application containers.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M5: Insufficient Cryptography
Review OWASP: M7: Client Code Quality
Review NIAP: FMT_CFG_EXT.1.2
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data

Test Performed

We scan the application code to look for usage of the MODE_WORLD_READABLE or MODE_WORLD_WRITEAB LE flags when storing files. Usage of these flags allows other applications and/or users on the device to acces s files stored with them. Developers should always use the MODE_PRIVATE flag when storing files on the syst em.

PASSED

Exploitable **Does not expose low risk sensitive information** dynamic
CVSS Score: 4.3 CWE-200

Threat Details

Sensitive information should be carefully reviewed to ensure it is only shared when absolutely necess ary. Kryptowire highlights ALL sensitive informatio n sent, including those to Apple, & the app develo per to ensure the user is aware of all connections. Sharing of device metadata and unique user IDs (a dvertising IDs, generic user identifiers, etc) can be used in conjunction with other collected data to tr ack users and identify them based off what seems to be innocuous information.

Regulations

Review OWASP: M7: Client Code Quality
Review NIAP: FPR_ANO_EXT.1.1
Review GDPR: Article 44 - General Principle for Transfers to Third Countries or International Organizations

Test Performed

We scan all network traffic generated during Dynamic Analysis for any sensitive information. This includes bo th plain text HTTP and encrypted HTTPS.

PASSED

Does not make phone calls

hybrid CVSS Score: 2.3

Threat Details

Access to this functionality should be carefully vett ed for need in the application's context. This perm ission allows calling without the user confirming t he call. This could be used to spoof phone calls, ini tiate calls to paid calling services to fraudulently c harge the user, and more.

Regulations

Review NIAP: FDP_DEC_EXT.1.1

Test Performed

We determine if the application requires the permission to call a phone number from the device.

PASSED

Does not contain code with improper SSL verification

static CVSS Score: 7.4

CWE-295

Threat Details

Communications over the network may be insecure. If the vulnerable class(es) are used any sensitive data transmitted to or from this application could be intercepted, altered, or stolen.

Regulations

Review OWASP: M3: Insecure Communication
Review OWASP: M7: Client Code Quality
Review NIAP: FCS_TLSC_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

Scans were performed on the application's byte code and any packaged SDKs to search for custom SSL managers that bypass proper SSL verification. These custom implementations should perform checks on the given certificate to determine if it is valid or not. The identified class returns no errors which therefore accept all SSL certificates. More information can be found here

PASSED

Exploitable **No unencrypted network connections made** dynamic CVSS Score: 6.3

CWE-5

Threat Details

If any sensitive data is exchanged over the network through the application it is essential to use encrypted network communications. If the application does not use encrypted connections the app should not have access to any sensitive functionality or data.

Regulations

Review OWASP: M3: Insecure Communication
Review OWASP: M7: Client Code Quality
Review NIAP: FTP_DIT_EXT.1.1
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data
Review GDPR: Article 25: Data Protection by Design and by Default

Test Performed

We check for the use of SSL/TLS encryption during web communications made by the application.

PASSED

Exploitable **App does not leak logs to public storage** hybrid CVSS Score: 5.7

CWE-312

Threat Details

Applications with this vulnerability may leak information from the application which contains sensitive user information and/or informs application internal functionality. User information may be exposed to other applications on the device. It is also possible that information about the applications internal functionality could be used to reverse engineer and/or attack the application and its backend.

Regulations

Review OWASP: M7: Client Code Quality
Review OWASP: M2: Insecure Data Storage
Review OWASP: M9: Reverse Engineering
Review GDPR: Article 32: Security of Processing
Review GDPR: Article 5: Principles Relating to Processing of Personal Data

Test Performed

We evaluate the application's usage of the Logcat command and determine if the application writes them to publically addressable storage location.

PASSED

Exploitable **SSL pinning detected** dynamic CVSS Score: 6.6 CWE-295

Threat Details

SSL pinning is an essential technique to help prevent man-in-the-middle attacks on backend connections. If it is not utilized it is possible for attackers to intercept, monitor, and change communications between the application and backend.

Regulations

Review OWASP: M3: Insecure Communication

Test Performed

We attempt to perform a man-in-the-middle attack on the backend connections and monitor for use of pinned SSL certificates.

PASSED

Exploitable **App does not contain a known medium-risk vulnerability** hybrid
CVSS Score: 5.5 CWE-829

Threat Details

A vulnerability was identified in a library packaged in the application. The severity and identifier of the specific vulnerability can be seen below.

Regulations

Review OWASP: M8: Code Tampering
Review OWASP: M9: Reverse Engineering

Test Performed

The application binary is processed through a dedicated library and SDK parsing engine which identifies the i ncluded libraries and SDKs by their code signatures. The engine also identifies the version of the artifact. This information is used to query for known CVEs associated with the library or SDK name and version. Full results are available in Kryptowire's Software-Bill-of-Materials (SBOM) report in the Kryptowire MAST Portal UI.

PASSED

Does not track user behaviour

dynamic | CVSS Score: 3.5

Threat Details

Users basic device information and behavior in th e application are being tracked. Users should ensu re this application developer is trustworthy to han dle this information. Developers should ensure th e tracking/analytics company is trustworthy and m eets their security and privacy standards.

Regulations

Review NIAP: FPR_ANO_EXT.1.1
Review GDPR: Article 44 - General Principle for Transfers to Third Countries or International Organizations
Review GDPR: Article 17: Right to be Forgotten

Test Performed

We scan through all network traffic generated by the application during Dynamic Analysis for the presence of tracking and/or analytics service traffic being transmitted.

PASSED

No ad network integration

dynamic | CVSS Score: 3.5

Threat Details

Integration with advertising networks allows for tr acking the user based off advertising identifiers an d device metadata. This information can be combi ned with other datasets in the backend to identify user behavior, preferences, locations, and more. S pecial attention should be given to advertisers bas ed in un-trusted countries.

Regulations

Review NIAP: FPR_ANO_EXT.1.1
Review GDPR: Article 44 - General Principle for Transfers to Third Countries or International Organizations
Review GDPR: Article 17: Right to be Forgotten
Review GDPR: Article 22: Automated Individual Decision-Making, Including Profiling

Test Performed

We scan through all network traffic generated by the application during Dynamic Analysis for the presence of Advertising Network traffic being transmitted.

No cloud storage integration

dynamic | CVSS Score: 3.5

PASSED

Threat Details

Integration with cloud storage services enables st orage of user files on the cloud. The type of data a ccessed by the app should be considered when as sessing the risk of this capability. If there is sensiti ve data access cloud storage with third parties cou ld be dangerous.

Regulations

Review NIAP: FPR_ANO_EXT.1.1

Review GDPR: Article 44 - General Principle for Transfers to Third Countries or International Organizations

Review GDPR: Article 17: Right to be Forgotten

Test Performed

We scan through all network traffic generated by the application during Dynamic Analysis for the presence of cloud storage traffic being transmitted.

No social network integration

dynamic | CVSS Score: 3.5

PASSED

Threat Details

Integration with social networks is common in con sumer applications and should be considered nor mal. For business applications that may contain se nsitive data connections to social networks should be reviewed for the data shared and purpose.

Regulations

Review NIAP: FPR_ANO_EXT.1.1

Review GDPR: Article 44 - General Principle for Transfers to Third Countries or International Organizations

Review GDPR: Article 17: Right to be Forgotten

Test Performed

We scan through all network traffic generated by the application during Dynamic Analysis for the presence of communication with know social networks.

No access to Account Manager

static CVSS Score: 2.8

PASSED

Threat Details

Access to user accounts on the device can give an application information about which other apps are installed on the device. The app gains access to an array of the accounts registered with the device including the creator, name, and type of account.

Regulations

Review NIAP: FDP_DEC_EXT.1.2

Test Performed

We identify any access by the application to Android's Account Manager which is used as a central location to store account information for various applications.

Does not access subscriber ID

dynamic CVSS Score: 3.3

PASSED

Threat Details

The subscriber ID allows the identification and tracking of the user and identification of the user's cellular provider.

Regulations

Review NIAP: FDP_DEC_EXT.1.2

Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject

Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We monitor the app during Dynamic Analysis for access to the getSubscriberId() method or the equivalent through other methods.

Does not access unique device ID

dynamic CVSS Score: 3.3

PASSED

Threat Details

The IMEI of the device is a unique ID that remains unchanged throughout the device's life. This ID allows identification and tracking of the specific hardware the application is installed on.

Regulations

Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We monitor the app during Dynamic Analysis for access to the getDeviceId() method or the equivalent through other methods.

PASSED

Does not access device SIM number

dynamic CVSS Score: 3.3

Threat Details

The SIM serial number allows identification and tracking of the user across services and identification of the user's cellular provider.

Regulations

Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We monitor the app during Dynamic Analysis for access to the getSimSerialNumber() method or the equivalent through other methods.

PASSED

Does not access device phone number

dynamic CVSS Score: 2.3

Threat Details

The phone number of the device allows identification and tracking of the user across services and can be used for spam, phishing attacks, or 2FA attacks.

Regulations

Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We monitor the app during Dynamic Analysis for access to the getLine1Number() method or the equivalent t hrough other methods.

PASSED

Does not access Bluetooth

hybrid | CVSS Score: 2.3

Threat Details

Access to all nearby bluetooth devices is granted with this permission. The application can search f or nearby devices and initiate connection.

Regulations

Review NIAP: FDP_DEC_EXT.1.1

Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject

Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We determine if the application requires permission for accessing the Bluetooth functionality of the device.

PASSED

Does not access NFC

static | CVSS Score: 2.3

Threat Details

Access to the NFC functionality allows the app to c ommunicate with any NFC device that is nearby to the device. This can include transmission of infor mation to other NFC enabled mobile phones or N FC storage chips. The range for NFC data transfer i s approximately 4cm.

Regulations

Review NIAP: FDP_DEC_EXT.1.1

Test Performed

We determine if the application requires permission for the NFC functionality of the device.

Does not access location

hybrid | CVSS Score: 2.3

PASSED

Threat Details

Access to the fine location of the user will give the application exact details of where the device is loc ated. The precision accuracy is approximately 3-5 m, typically this allows the app to see where the u ser is down to a specific address or building.

Regulations

Review NIAP: FDP_DEC_EXT.1.1
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We determine if the application requires permission to access the device's physical location.

Does not access calendar

hybrid CVSS Score: 2.3

PASSED

Threat Details

Access to write user's calendar data should be con sidered dangerous. The application has no restrict ions for the type of events it can create and could trick the user with fake calendar events or modific ations to existing calendar events.

Regulations

Review NIAP: FDP_DEC_EXT.1.2
Review GDPR: Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject
Review GDPR: Article 6: Lawfulness of Processing

Test Performed

We determine if the application requires the permission(s) to read and or write to the device's calendar.

Does not have leftover files after uninstall

dynamic CVSS Score: 3.3

PASSED

Threat Details

Files that remain on the device after the applicatio n is removed may expose data about the user an d/or application.

Regulations

Review OWASP: M2: Insecure Data Storage
Review OWASP: M7: Poor Code Quality
Review NIAP: FPT_TUD_EXT.2.2

Test Performed

We monitor the application during dynamic analysis for files created to the external storage, not the private a pplication directory. These files persist on the device after the application is removed.

PASSED

Exploitable **App does not contain a known low-risk vulnerability** hybrid

CVSS Score: 2.1 CWE-829

Threat Details

A vulnerability was identified in a library packaged in the application. The severity and identifier of th e specific vulnerability can be seen below.

Regulations

Review OWASP: M8: Code Tampering

Review OWASP: M9: Reverse Engineering

Test Performed

The application binary is processed through a dedicated library and SDK parsing engine which identifies the i ncluded libraries and SDKs by their code signatures. The engine also identifies the version of the artifact. This information is used to query for known CVEs associated with the library or SDK name and version. Full results are available in Kryptowire's Software-Bill-of-Materials (SBOM) report in the Kryptowire MAST Portal UI.

Application Information

Application name	Package name
InsecureShop	com.insecureshop
Application version	**Number of permissions requested**
1.0	5
MD5 hash	**SHA1 hash**
c3b65406a80b9685a548e3e927fbefdd	5a68ca276a1003db3677bcd206b1f4b9bc5caa81
Min SDK version	**Target SDK version**
16	29

Permissions Requested

android.permission.INTERNET
android.permission.READ_CONTACTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE

Libraries Used

None declared

Features Used

None declared

AV Scan Results

Clean

App Protection Analysis

No Protection Found

Sensitive Data Exposure

No sensitive data exposure detected

No issues found

SSL Pinning Data

No SSL Connections

Network Traffic

No network traffic captured

Quokka

Appendix

Standard	Description	Details
Threat Score	The threat score is based on the types of issues that were found during analysis.	The threat score is a combination of the number of issues found and their risk level. If you have customized your threat score profile, those changes will be reflected in the threat score. Low Risk: below 35 Medium Risk: Between 35 and 75 High Risk: Above 75
OWASP	Represents a broad consensus about the most critical security risks to applications	We analyze the app and provide score based on Top 10 OWASP Mobile Risks
NIAP	A U.S. Government initiative established to promote the use of evaluated information systems products and champion the development and use of national and international standards for information technology security	We analyzed the app and provide score based on NIAP Protection Profile for Application Software
GDPR	A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA)	We analyzed the app and provide score based on GDPR Articles