ANDROID STATIC ANALYSIS REPORT

GALAXYAPP V3 (1.0.10)

File Name:	NMI_DOM_UAT_07072025.apk
Package Name:	com.BIAL.GalaxyV3
Scan Date:	July 24, 2025, 6:40 a.m.
App Security Score:	36/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
5	7	1	1	1

FILE INFORMATION

File Name: NMI_DOM_UAT_07072025.apk
Size: 5.88MB
MD5: a0accdd6d2d3ac24f1496ed8c07ee275
SHA1: 42b6b86faceebfcb375af84da791bdf87abf1f16
SHA256: 41e3d367c93665cfeaaa83d77e477923c681de4e716351c7ad810e6ad70696b2

APP INFORMATION

App Name: GALAXYAPP V3
Package Name: com.BIAL.GalaxyV3
Main Activity: com.BIAL.GalaxyV3.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 1.0.10
Android Version Code: 10010

APP COMPONENTS

Activities: 1
Services: 0
Receivers: 0
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=91, ST=Maharashtra, L=Mumbai, O=Kale Logistics Solutions Pvt Ltd., OU=Kale Logistics, CN=Sachin Semlety
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-10-01 11:10:51+00:00
Valid To: 2118-09-07 11:10:51+00:00
Issuer: C=91, ST=Maharashtra, L=Mumbai, O=Kale Logistics Solutions Pvt Ltd., OU=Kale Logistics, CN=Sachin Semlety
Serial Number: 0x3a5fa76f
Hash Algorithm: sha256
md5: ffe28c728da1a3945661caf1f4725b7f
sha1: cb3245d7abc137d66baa5acd199378eb5e245836
sha256: f67fd8a914bbe410f5ce30de159838a6f2f77ecd35d2732ba0cf79acad240bd5
sha512: e87980bfeaec69daf1637b3cbd5b210e1a5e1dc79bfcf8244f93cf496f8270aaa3b3f4d79bf951372e15417f41af63967fa364a18cc288c2c1e9014af6ec52d0
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8bb905016329e38a0fa5d72a6bed2795b304e2694562542abdea7c84b6980c71
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
com.BIAL.GalaxyV3.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

HIGH: **2** | WARNING: **1** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	https://gmrintluat.kalelogistics.com:7081/	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **1** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

CODE ANALYSIS

HIGH: **1** | WARNING: **4** | INFO: **1** | 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	com/datecs/api/emsr/EMSR.java com/datecs/api/hub/HUB.java com/datecs/api/linea/LineaPro.java com/datecs/api/linea/LineaProInformation.java com/datecs/api/printer/Printer.java com/datecs/api/printer/ProtocolAdapter.java com/datecs/api/rfid/RFID.java com/datecs/api/universalreader/UniversalReader.java com/giorgiofellipe/datecsprinter/DatecsSDKWrapper.java com/giorgiofellipe/datecsprinter/Printer.java com/github/diegorquera/zbtprinter/ZebraBluetoothPrinter.java com/zebra/sdk/printer/internal/VerbosePrinter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/zebra/sdk/printer/discovery/internal/FindPrinters.java com/zebra/sdk/printer/discovery/internal/LocalBroadcast.java com/zebra/sdk/printer/discovery/internal/MulticastBroadcast.java com/zebra/sdk/printer/internal/PortStatus.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/zebra/sdk/printer/internal/ProfileHelper.java com/zebra/sdk/printer/internal/ProfileUtilLinkOsImpl.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/datecs/api/rfid/ISO14443Card.java
5	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/datecs/api/rfid/ISO14443Card.java
6	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/zebra/sdk/comm/internal/FTP.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/datecs/api/hub/HUB.java com/zebra/sdk/printer/FontConverterZpl.java com/zebra/sdk/printer/internal/ZebraFileConnectionImpl.java com/zebra/sdk/printer/internal/ZebraPrinterLinkOsImpl.java com/zebra/sdk/util/internal/Base64.java com/zebra/sdk/util/internal/FileReader.java com/zebra/sdk/util/internal/FontConverterHelper.java com/zebra/sdk/util/internal/ZipUtil.java
00162	Create InetSocketAddress object and connecting to it	socket	com/zebra/sdk/comm/internal/ZebraNetworkSocket.java
00163	Create new Socket and connecting to it	socket	com/zebra/sdk/comm/internal/ZebraNetworkSocket.java
00012	Read data and put it into a buffer stream	file	com/zebra/sdk/util/internal/Base64.java com/zebra/sdk/util/internal/ZipUtil.java
00022	Open a file from given absolute path of the file	file	com/zebra/sdk/printer/internal/ProfileHelper.java com/zebra/sdk/printer/internal/ProfileUtilLinkOsImpl.java com/zebra/sdk/util/internal/FileReader.java com/zebra/sdk/util/internal/FileWrapper.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_PHONE_STATE
Other Common Permissions	2/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

HARDCODED SECRETS

POSSIBLE SECRETS
7a5b85d3ee2e0991ca3502602e9389a98f55c0576b887125894a7ec03823f8d3

SCAN LOGS

Timestamp	Event	Error
2025-07-24 06:40:45	Generating Hashes	OK

2025-07-24 06:40:45	Extracting APK	OK
2025-07-24 06:40:45	Unzipping	OK
2025-07-24 06:40:45	Parsing APK with androguard	OK
2025-07-24 06:40:45	Extracting APK features using aapt/aapt2	OK
2025-07-24 06:40:45	Getting Hardcoded Certificates/Keystores	OK
2025-07-24 06:40:49	Parsing AndroidManifest.xml	OK
2025-07-24 06:40:49	Extracting Manifest Data	OK
2025-07-24 06:40:49	Manifest Analysis Started	OK
2025-07-24 06:40:49	Reading Network Security config from network_security_config.xml	OK
2025-07-24 06:40:49	Parsing Network Security config	OK
2025-07-24 06:40:49	Performing Static Analysis on: GALAXYAPP V3 (com.BIAL.GalaxyV3)	OK

2025-07-24 06:40:50	Fetching Details from Play Store: com.BIAL.GalaxyV3	OK
2025-07-24 06:40:50	Checking for Malware Permissions	OK
2025-07-24 06:40:50	Fetching icon path	OK
2025-07-24 06:40:50	Library Binary Analysis Started	OK
2025-07-24 06:40:50	Reading Code Signing Certificate	OK
2025-07-24 06:40:51	Running APKiD 2.1.5	OK
2025-07-24 06:40:54	Updating Trackers Database....	OK
2025-07-24 06:40:54	Detecting Trackers	OK
2025-07-24 06:40:55	Decompiling APK to Java with JADX	OK
2025-07-24 06:41:18	Converting DEX to Smali	OK

2025-07-24 06:41:18	Code Analysis Started on - java_source	OK
2025-07-24 06:41:19	Android SBOM Analysis Completed	OK
2025-07-24 06:41:20	Android SAST Completed	OK
2025-07-24 06:41:20	Android API Analysis Started	OK
2025-07-24 06:41:21	Android API Analysis Completed	OK
2025-07-24 06:41:22	Android Permission Mapping Started	OK
2025-07-24 06:41:24	Android Permission Mapping Completed	OK
2025-07-24 06:41:24	Android Behaviour Analysis Started	OK
2025-07-24 06:41:25	Android Behaviour Analysis Completed	OK
2025-07-24 06:41:25	Extracting Emails and URLs from Source Code	OK
2025-07-24 06:41:25	Email and URL Extraction Completed	OK

2025-07-24 06:41:25	Extracting String data from APK	OK
2025-07-24 06:41:25	Extracting String data from Code	OK
2025-07-24 06:41:25	Extracting String values and entropies from Code	OK
2025-07-24 06:41:26	Performing Malware check on extracted domains	OK
2025-07-24 06:41:26	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.