ANDROID STATIC ANALYSIS REPORT

app_icon

Proyecto_yeis2 (1.0)

File Name:	app-debug.apk
Package Name:	prototype.proyecto_yeis2
Scan Date:	Oct. 24, 2024, 8:19 p.m.
App Security Score:	36/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
3	2	0	1	0

FILE INFORMATION

File Name: app-debug.apk
Size: 5.83MB
MD5: 7fa03b96dcb1b39e252f67e06557899b
SHA1: 7e47df32adcc3f5993097d4539d7a3fa517f771b
SHA256: 6f26f94cb08f219507e0da4c922515d95485ac99b17141f265a7f27d7f41c8ec

APP INFORMATION

App Name: Proyecto_yeis2
Package Name: prototype.proyecto_yeis2
Main Activity: prototype.proyecto_yeis2.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

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

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-09-11 01:21:22+00:00
Valid To: 2054-09-04 01:21:22+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 3404f05e639e28d15845a9926e5d7305
sha1: 8a3fd804dea62a908d5ff594d611956ff6142fe3
sha256: 92d292669625021725784d1f0c313082cfa0bc680be9cc6dd2017c58970c4a99
sha512: 740f3ff65840511756886ec1c6445f2b49c87229a78c3ee6a0cafc474766e83b3142e8510507602e678a497d3230ad358bde704a49d3ff35dbd4d5793f0b4279
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 166c02ea55e72128c25e1441680bfa29a8a8958d642a2e911d12a5826ab52bc0
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
prototype.proyecto_yeis2.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>classes3.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
<tr><td>classes4.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
<tr><td>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table></td></tr>
</table>

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	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

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/24	
Other Common Permissions	0/45	

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

SCAN LOGS

Timestamp	Event	Error
2024-10-24 20:19:14	Performing Malware check on extracted domains	OK
2024-10-24 20:19:14	Saving to Database	OK

2024-10-24 20:19:20	Converting DEX to Smali	OK
2024-10-24 20:19:20	Code Analysis Started on - java_source	OK
2024-10-24 20:19:21	Android SAST Completed	OK
2024-10-24 20:19:21	Android API Analysis Started	OK
2024-10-24 20:19:26	Android Permission Mapping Started	OK
2024-10-24 20:19:26	libsast scan failed	AttributeError("'NoneType' object has no attribute 'values'")
2024-10-24 20:19:26	Android Permission Mapping Completed	OK
2024-10-24 20:19:27	Finished Code Analysis, Email and URL Extraction	OK
2024-10-24 20:19:27	Extracting String data from APK	OK
2024-10-24 20:19:28	Extracting String data from Code	OK
2024-10-24 20:19:28	Extracting String values and entropies from Code	OK

2024-10-24 20:19:34	Performing Malware check on extracted domains	OK
2024-10-24 20:19:34	Saving to Database	OK
2024-10-24 20:20:07	Converting DEX to Smali	OK
2024-10-24 20:20:07	Code Analysis Started on - java_source	OK
2024-10-24 20:20:13	Android SAST Completed	OK
2024-10-24 20:20:13	Android API Analysis Started	OK
2024-10-24 20:20:22	Android Permission Mapping Started	OK
2024-10-24 20:20:23	libsast scan failed	AttributeError("'NoneType' object has no attribute 'values'")
2024-10-24 20:20:23	Android Permission Mapping Completed	OK
2024-10-24 20:20:24	Finished Code Analysis, Email and URL Extraction	OK
2024-10-24 20:20:24	Extracting String data from APK	OK

2024-10-24 20:20:24	Converting DEX to Smali	OK
2024-10-24 20:20:25	Code Analysis Started on - java_source	OK
2024-10-24 20:20:26	Extracting String data from Code	OK
2024-10-24 20:20:26	Extracting String values and entropies from Code	OK
2024-10-24 20:20:46	Performing Malware check on extracted domains	OK
2024-10-24 20:20:46	Saving to Database	OK

Report Generated by - MobSF v4.0.7

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.