


Findings		
	High 2	
	Medium 15	
	Info 3	
	Secure 1	
	Hotspot 1	
<div>high</div> App can be installed on a vulnerable upatched Android version		MANIFEST
<div>high</div> Application contains Privacy Trackers		TRACKERS
<div>medium</div> Application vulnerable to Janus Vulnerability		CERTIFICATE
<div>medium</div> Application Data can be Backed up		MANIFEST
<div>medium</div> Activity (com.crowdin.platform.auth.AuthActivity) is not Protected.		MANIFEST
<div>medium</div> Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.		MANIFEST
<div>medium</div> Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.		MANIFEST
<div>medium</div> Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.		MANIFEST
<div>medium</div> Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.		MANIFEST
<div>medium</div> Files may contain hardcoded sensitive information like usernames, passwords, keys etc.		CODE
<div>medium</div> The App uses an insecure Random Number Generator.		CODE
<div>medium</div> App can read/write to External Storage. Any App can read data written to External Storage.		CODE
<div>medium</div> SHA-1 is a weak hash known to have hash collisions.		CODE
		CODE

medium	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.	
medium	App creates temp file. Sensitive information should never be written into a temp file.	CODE
medium	MD5 is a weak hash known to have hash collisions.	CODE
medium	This app may contain hardcoded secrets	SECRETS
info	The App logs information. Sensitive information should never be logged.	CODE
info	App can write to App Directory. Sensitive Information should be encrypted.	CODE
info	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	CODE
secure	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
hotspot	Found 4 critical permission(s)	PERMISSIONS

MobSF Application Security Scorecard generated for  (mSpy Installer 1.2.0) 