






Findings		
	High 2	
	Medium 23	
	Info 1	
	Secure 1	
	Hotspot 1	
<div><div>high</div>App can be installed on a vulnerable upatched Android version</div>		MANIFEST
<div><div>high</div>The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.</div>		CODE
<div><div>medium</div>Application vulnerable to Janus Vulnerability</div>		CERTIFICATE
<div><div>medium</div>Launch Mode of activity (com.awti.slc.installer.MainActivity) is not standard.</div>		MANIFEST
<div><div>medium</div>Launch Mode of activity (com.awti.slc.installer.LoginActivity) is not standard.</div>		MANIFEST
<div><div>medium</div>Service (com.awti.slc.client.WWFObserverService) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.awti.slc.client.BootBroadcastReceiver) is not Protected.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.awti.slc.client.ShutdownBroadcastReceiver) is not Protected.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.awti.slc.client.StillRunningBroadcastReceiver) is not Protected.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.awti.slc.client.PackageAddedReceiver) is not Protected.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.awti.slc.client.UninstallProtectionReceiver) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.awti.slc.client.SMSBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.</div>		MANIFEST
<div><div>medium</div>Broadcast Receiver (com.awti.slc.client.MediaStatusBroadcastReceiver) is not Protected.</div>		MANIFEST
		MANIFEST

medium	Broadcast Receiver (com.awti.slc.client.AppMonitorBroadcastReceiver) is not Protected.	
medium	Broadcast Receiver (com.awti.slc.client.ScreenshotReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.awti.slc.client.MessageHandler) is not Protected.	MANIFEST
medium	Service (com.awti.messaging.MessagingService) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	MD5 is a weak hash known to have hash collisions.	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.	CODE
medium	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	SHA-1 is a weak hash known to have hash collisions.	CODE
medium	The App uses an insecure Random Number Generator.	CODE
medium	Application contains Privacy Trackers	TRACKERS
medium	This app may contain hardcoded secrets	SECRETS
info	The App logs information. Sensitive information should never be logged.	CODE
secure	This App may have root detection capabilities.	CODE
hotspot	Found 16 critical permission(s)	PERMISSIONS