ANDROID STATIC ANALYSIS REPORT

EU Mobile Money (1.18)

File Name:	com.eusa.english.home_2020-04-27.apk
Package Name:	com.eusa.english.home
Average CVSS Score:	5.8
App Security Score:	40/100 (HIGH RISK)
Trackers Detection:	2/285

FILE INFORMATION

File Name: com.eusa.english.home_2020-04-27.apk
Size: 6.77MB
MD5: e0411e04be6253f3fb47dbb27af13f4d
SHA1: 26dcb603c315331ac9e693e760a1775a63d9a526
SHA256: 1acba7159f0f654bc565e47e1f35ce392e5c3831b1cb98f4f7c1d80891da87e2

APP INFORMATION

App Name: EU Mobile Money
Package Name: com.eusa.english.home
Main Activity: estel.eu_agent.Miscelineous.SplashActivity
Target SDK: 28
Min SDK: 14
Max SDK:
Android Version Name: 1.18
Android Version Code: 19

APP COMPONENTS

Activities: 77
Services: 5
Receivers: 4
Providers: 2
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=IN, ST=haryana, L=gurgaon, O=Estel Technologies Pvt. Ltd., OU=Mobile Apps, CN=Aditya Bugalia
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-11-06 07:13:08+00:00
Valid To: 2039-10-31 07:13:08+00:00
Issuer: C=IN, ST=haryana, L=gurgaon, O=Estel Technologies Pvt. Ltd., OU=Mobile Apps, CN=Aditya Bugalia
Serial Number: 0x545b1f84
Hash Algorithm: sha1
md5: 0a3634a126f524365054542f2580a9cc
sha1: 1b55685c7af2c0160069fad8ed822dfba97a6817
sha256: 179b95bb11f87de65126c07f6143efaff191871b5339ae7f832396a17f05ce14
sha512:
c63188bd8bf34a70c053baed553d4d2b271eb5fbd198138fa4d17cb5026acd3e49a0d3e0f86b5324fb29ba31d7c60e943efea88dd05c8d295e63681063b3a642

PublicKey Algorithm: rsa

Bit Size: 1024
Fingerprint: 51ca556d68a4b46d18d1bf1463a0eda360c1fe6b601757806bc90aa2aead09ef

Certificate Status: Bad
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti Debug Code — DETAILS: Debug.isDebuggerConnected() check FINDINGS: Anti-VM Code — DETAILS: Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check

	Build.TAGS check
Compiler	dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
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.
App has a Network Security Configuration [android:networkSecurityConfig]	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.
Broadcast Receiver (estel.eu_agent.OTP.OTPRecieverGlobal) is not Protected. [android:exported=true]	high	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.
Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	high	A Service 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.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	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.
Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	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.
Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			estel/eu_agent/Tariff/QuickTariff.java estel/eu_agent/Tariff/Tariff.java estel/eu_agent/Tariff/TariffSelectionActivity.java estel/eu_agent/cash_deposit_withdraw/CashWithdrawInitiateActiviy.java estel/eu_agent/cash_deposit_withdraw/CashWithdrawDepositSelectorActivity.java estel/eu_agent/cash_deposit_withdraw/CashDepositActivity.java estel/eu_agent/BillPay/BillPayIntroduction.java estel/eu_agent/BillPay/BillPayFinal.java estel/eu_agent/BillPay/BillPaymentActivity.java estel/eu_agent/BillPay/NewBillPaymentActivity.java estel/eu_agent/accountmanagement/MiniReportActivity.java estel/eu_agent/accountmanagement/MobileServiceBankingActivation.java estel/eu_agent/accountmanagement/AccountManagement.java estel/eu_agent/accountmanagement/InterestOnMobileAccount.java estel/eu_agent/accountmanagement/CustomerService.java estel/eu_agent/accountmanagement/a.java estel/eu_agent/accountmanagement/StatementsSelectorActivity.java estel/eu_agent/accountmanagement/ChangeMpinActivity.java estel/eu_agent/accountmanagement/RemoveAccountActivity.java estel/eu_agent/accountmanagement/Balance

The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	CheckActivity.java estel/eu_agent/loans/LoanSelectorActivity.java estel/eu_agent/loans/loan_status/a.java estel/eu_agent/loans/loan_status/LoanStatusDisplayActivity.java estel/eu_agent/loans/loan_repayment/LoanRepaymentFinalActivity.java estel/eu_agent/loans/loan_repayment/a.java estel/eu_agent/loans/loan_repayment/AutomaticLoanRepaymentActivity.java estel/eu_agent/loans/loan_request/LoanRequestActivity.java estel/eu_agent/loans/loan_subscribe/LoanRegistrationActivity.java estel/eu_agent/loans/loan_gurantor/manage_guarantor/ManageGuarantorFinalActivity.java estel/eu_agent/loans/loan_gurantor/manage_guarantor/a.java estel/eu_agent/loans/loan_gurantor/manage_guarantor/AutomaticManageguarantorActivity.java estel/eu_agent/loans/loan_gurantor/add_gurantor/AddGurantorActivity.java estel/eu_agent/loans/loan_gurantor/approve_guarantor/ApproveGuarantorFinalActivity.java estel/eu_agent/loans/loan_gurantor/approve_guarantor/a.java estel/eu_agent/loans/loan_gurantor/approve_guarantor/AutomaticApproveGuarantorActivity.java estel/eu_agent/loans/loan_gurantor/guarantor_common/LoanGuranterActivity.java estel/eu_agent/PaymentAuth/AutomaticPaymentAuth/PaymentAuthFinalActivity.java estel/eu_agent/PaymentAuth/AutomaticPaymentAuth/PaymentAuthAutomaticActivity.java estel/eu_agent/PaymentAuth/OnlinePaymentAuth/PaymentAuthOnlineActivity.java estel/eu_agent/PaymentAuth/CommonInterfacePaymentAuth/PaymentAuthTypeSelectorActivity.java estel/eu_agent/PaymentAuth/CommonInterfacePaymentAuth/CommonPaymentAuthReviewActivity.java estel/eu_agent/PaymentAuth/ManualPaymentAuth/PaymentAuth.java estel/eu_agent/purchase_goods_services/PrepaidElectricityBillPayment.java estel/eu_agent/purchase_goods_services/PurchaseActivity.java estel/eu_agent/purchase_goods_services/GeneratePaymentCode.java estel/eu_agent/purchase_goods_services/PurchaseGoodsServicesGenerateCodeActivity.java estel/eu_agent/PaymentTransfer/PaymentTransferActivity.java estel/eu_agent/Miscelineous/InterestEarned.java estel/eu_agent/Miscelineous/LoginActivity.java

				estel/eu_agent/Miscelineous/SplashActivity.java estel/eu_agent/qr_code/d.java estel/eu_agent/qr_code/a.java estel/eu_agent/qr_code/QR_PurchaseActivity.java estel/eu_agent/moneytransfer/MoneyTransferActivity.java estel/eu_agent/moneytransfer/MoneyTransferActivity_New.java estel/eu_agent/moneytransfer/CashToAccount/CashToAccountActivity.java estel/eu_agent/moneytransfer/AccountToAccount/AccountToAccountActivity.java estel/eu_agent/moneytransfer/AccountToCash/AccountToCashActivity.java estel/eu_agent/OTP/OTPVerificationActivity.java f/b.java d/a/a/a/a.java tutionfees_fragment/b.java tutionfees_fragment/TutionFeesMenu.java tutionfees_fragment/d.java tutionfees_fragment/c.java tutionfees_fragment/SucessReceiptTutionFees.java tutionfees_fragment/e.java tutionfees_fragment/a.java tutionfees_fragment/TutionFeesAcitivity.java c/a/a/a/b.java c/a/a/a/a/c/a.java c/a/a/a/a/b/x.java activation/GenerateOTPActivity.java purchase_billpayment_deposit/PurchaseBillPaymentDepositMenu.java com/a/a/v.java b/b.java eui/SendMoneyCashtoMobileCashtoCashMenu.java eui/printer_utilities/b.java eui/printer_utilities/a.java eui/printer_utilities/PrinterListShowActivity.java eui/receivemoney_cashtocash_fragment/b.java eui/receivemoney_cashtocash_fragment/SuccessReceiptCashToReceive.java eui/receivemoney_cashtocash_fragment/d.java eui/receivemoney_cashtocash_fragment/c.java eui/receivemoney_cashtocash_fragment/ReceiveMoneyCashToCashDiffrentCountryActivity.java eui/receivemoney_cashtocash_fragment/h.java eui/receivemoney_cashtocash_fragment/f.java eui/sendmoney_cashtocash_fragment/b.java eui/sendmoney_cashtocash_fragment/DiffrentCountrySendMoneyActivity.java eui/sendmoney_cashtocash_fragment/SucessReceiptCashToCashSendMoney.java eui/sendmoney_cashtocash_fragment/c.java eui/sendmoney_cashtocash_fragment/i.java

			eui/sendmoney_cashtocash_fragment/k.java eui/sendmoney_cashtocash_fragment/a.java eui/sendmoney_cashtocash_fragment/g.java eui/sendmoney_cashtocash_fragment/h.java eui/sendmoney_cashtocash_fragment/j.java eui/sendmoney_cashtocash_fragment/f.java commonutilities/c.java commonutilities/e.java commonutilities/ComponentInfo.java commonutilities/h.java commonutilities/j.java
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	estel/eu_agent/Tariff/QuickTariff.java estel/eu_agent/Tariff/Tariff.java estel/eu_agent/Miscelineous/LoginActivity.java estel/eu_agent/Miscelineous/DisplayActivity.java estel/eu_agent/OTP/OTPVerificationActivity.java c/a/a/a/c.java c/a/a/a/a/b/b.java com/a/a/n.java com/a/a/g.java com/a/a/a/e.java com/b/a/a/a.java commonutilities/e.java
IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor OWASP MASVS: MSTG-CODE-2	c/a/a/a/c.java c/a/a/a/m.java
This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	c/a/a/a/a/b/i.java
The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 (high) CWE: CWE-330 - Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	activation/GenerateOTPActivity.java
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.	high	CVSS V2: 5.9 (medium) CWE: CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	b/a.java
MD5 is a weak hash known to have hash collisions.	high	CVSS V2: 7.4 (high) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	commonutilities/ComponentInfo.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
e.crashlytics.com	good	IP: 54.243.112.173 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.04372 Longitude: -77.487488 View: Google Map
www.expressunion.net	good	IP: 149.202.217.128 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.69421 Longitude: 3.17456 View: Google Map
settings.crashlytics.com	good	IP: 108.177.119.94 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
eu-subscriber-app.firebaseio.com	good	IP: 35.201.97.85 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
play.google.com	good	IP: 172.217.218.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
wsdev.expressunion.net	good	IP: 213.251.146.177 Country: France Region: Ile-de-France City: Paris Latitude: 48.853409 Longitude: 2.3488 View: Google Map
expressunion.cm	good	IP: 213.186.50.179 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.69421 Longitude: 3.17456 View: Google Map

URLS

URL	FILE
https://play.google.com/store/apps/details?id=com.eusa.english.home http://www.expressunion.net/privacy-policy-for-users-of-mobile-money-apps/	estel/eu_agent/accountmanagement/AccountManagement.java
https://play.google.com/store/apps/details?id=com.eusa.english.home	estel/eu_agent/accountmanagement/CustomerService.java
https://play.google.com/store/apps/details?id=com.eusa.english.home	estel/eu_agent/Miscelineous/SplashActivity.java
https://e.crashlytics.com/spi/v2/events	c/a/a/a/a/g/k.java
https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings	c/a/a/a/a/g/q.java
https://wsdev.expressunion.net/transfinapiws/transactions/pay-out/	eui/sendmoney_cashtocash_fragment/b.java
https://wsdev.expressunion.net/transfinapiws/transactions/pay-out/	eui/sendmoney_cashtocash_fragment/c.java
http://expressunion.cm:5051/RESTfulWebServiceEU/json/estel/ https://eu-subscriber-app.firebaseio.com http://expressunion.cm:5051/TnC/termsandconditions_	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://eu-subscriber-app.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
foo@example.com bar@example.com	estel/eu_agent/Miscelineous/ApplicationSetupActivity.java

TRACKERS

TRACKER	URL
Google CrashLytics	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: EU Mobile Money

Score: 3.38 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 4.0 and up **Category:** Finance **Play Store URL:** com.eusa.english.home

Developer Details: EXPRESS UNION, EXPRESS+UNION, None, http://www.expressunion.net, info@expressunion.net,

Release Date: Jul 20, 2016 **Privacy Policy:** Privacy link

Description:

- Transfert d'argent; - Paiement de facture; - Gestion de compte; - Achat de Biens & Services.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.9 Beta

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.