APK Static Analysis Report

SSL/TLS Misconfigurations

Method: getDefaultSSLSocketFactory
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setRequestMethod
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setUseCaches
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setDoInput
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setDoOutput
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: getOutputStream
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setRequestProperty
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: connect
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: getResponseCode
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: getErrorStream
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: getInputStream
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: disconnect
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setConnectTimeout
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setReadTimeout
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setInstanceFollowRedirects
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: setSSLSocketFactory
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: getServerCertificates
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: getURL
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: createSocket
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: createSocket
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: createSocket
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: createSocket
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: createSocket
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: createSocket
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: getDefaultCipherSuites
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: getSupportedCipherSuites
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: addHandshakeCompletedListener
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: bind
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: close
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: connect
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: connect
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getChannel
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getEnableSessionCreation
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getEnabledCipherSuites
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getEnabledProtocols
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getInetAddress
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getInputStream
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getKeepAlive
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getLocalAddress
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getLocalPort
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getLocalSocketAddress
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getNeedClientAuth
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getOOBInline
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getOutputStream
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getPort
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getReceiveBufferSize
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getRemoteSocketAddress
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getReuseAddress
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSendBufferSize
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSession
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSoLinger
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSoTimeout
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSupportedCipherSuites
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSupportedProtocols
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getTcpNoDelay
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getTrafficClass
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getUseClientMode
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getWantClientAuth
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: isBound
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: isClosed
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: isConnected
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: isInputShutdown
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: isOutputShutdown
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: removeHandshakeCompletedListener
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: sendUrgentData
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setEnableSessionCreation
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setEnabledCipherSuites
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setEnabledProtocols
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setKeepAlive
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setNeedClientAuth
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setOOBInline
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setPerformancePreferences
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setReceiveBufferSize
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setReuseAddress
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setSendBufferSize
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setSoLinger
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setSoTimeout
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setTcpNoDelay
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setTrafficClass
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setUseClientMode
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setWantClientAuth
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: shutdownInput
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: shutdownOutput
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: startHandshake
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: toString
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSSLParameters
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setSSLParameters
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getApplicationProtocol
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getSocketFactory
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: init
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: getProvider
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: getDefaultAlgorithm
Class: Ljavax/net/ssl/TrustManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljavax/net/ssl/TrustManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: init
Class: Ljavax/net/ssl/TrustManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getTrustManagers
Class: Ljavax/net/ssl/TrustManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljavax/net/ssl/TrustManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getProvider
Class: Ljavax/net/ssl/TrustManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljavax/net/ssl/SSLPeerUnverifiedException;
Description: Potential SSL/TLS misuse detected

Method: initCause
Class: Ljavax/net/ssl/SSLPeerUnverifiedException;
Description: Potential SSL/TLS misuse detected

Method: verify
Class: Ljavax/net/ssl/HostnameVerifier;
Description: Potential SSL/TLS misuse detected

Method: getPeerCertificates
Class: Ljavax/net/ssl/SSLSession;
Description: Potential SSL/TLS misuse detected

Method: getCipherSuite
Class: Ljavax/net/ssl/SSLSession;
Description: Potential SSL/TLS misuse detected

Method: getLocalCertificates
Class: Ljavax/net/ssl/SSLSession;
Description: Potential SSL/TLS misuse detected

Method: getProtocol
Class: Ljavax/net/ssl/SSLSession;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljavax/net/ssl/SSLException;
Description: Potential SSL/TLS misuse detected

Method: getAcceptedIssuers
Class: Ljavax/net/ssl/X509TrustManager;
Description: Potential SSL/TLS misuse detected

Method: checkServerTrusted
Class: Ljavax/net/ssl/X509TrustManager;
Description: Potential SSL/TLS misuse detected

Method: getDefaultAlgorithm
Class: Ljavax/net/ssl/KeyManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljavax/net/ssl/KeyManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljavax/net/ssl/KeyManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getProvider
Class: Ljavax/net/ssl/KeyManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: init
Class: Ljavax/net/ssl/KeyManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getKeyManagers
Class: Ljavax/net/ssl/KeyManagerFactory;
Description: Potential SSL/TLS misuse detected

Method: getCause
Class: Ljavax/net/ssl/SSLHandshakeException;
Description: Potential SSL/TLS misuse detected

Method: getMessage
Class: Ljavax/net/ssl/SSLHandshakeException;
Description: Potential SSL/TLS misuse detected

Method: setApplicationProtocols
Class: Ljavax/net/ssl/SSLParameters;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljava/security/cert/CertificateFactory;
Description: Potential SSL/TLS misuse detected

Method: generateCertificate
Class: Ljava/security/cert/CertificateFactory;
Description: Potential SSL/TLS misuse detected

Method: getPublicKey
Class: Ljava/security/cert/Certificate;
Description: Potential SSL/TLS misuse detected

Method: getEncoded
Class: Ljava/security/cert/Certificate;
Description: Potential SSL/TLS misuse detected

Method: getType
Class: Ljava/security/cert/Certificate;
Description: Potential SSL/TLS misuse detected

Method: getSubjectX500Principal
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: getPublicKey
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: getSubjectDN
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: getSubjectAlternativeNames
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: getIssuerX500Principal
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: verify
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: getIssuerDN
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: equals
Class: Ljava/security/cert/X509Certificate;
Description: Potential SSL/TLS misuse detected

Method: getMessage
Class: Ljava/security/cert/CertificateException;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljava/security/cert/CertificateException;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljava/security/cert/CertificateException;
Description: Potential SSL/TLS misuse detected

Method: getMessage
Class: Ljava/security/cert/CertificateEncodingException;
Description: Potential SSL/TLS misuse detected

Method: getTrustedCert
Class: Ljava/security/cert/TrustAnchor;
Description: Potential SSL/TLS misuse detected

Cryptographic Misuse

Method: DES3
Class: Lcom/konasl/konapayment/sdk/i0/a/e/a;
Description: Use of weak cryptographic algorithm: DES

Method: DES3
Class: Lcom/konasl/konapayment/sdk/konaprepay/crypto/a;
Description: Use of weak cryptographic algorithm: DES

Method: DES3
Class: Lcom/mastercard/api/crypto/b;
Description: Use of weak cryptographic algorithm: DES

Method: SHA1
Class: Lcom/mastercard/api/crypto/b;
Description: Use of weak cryptographic algorithm: SHA1

Method: DES3
Class: Lcom/konasl/konapayment/sdk/i0/a/e/b;
Description: Use of weak cryptographic algorithm: DES

Method: DES3
Class: Lcom/konasl/konapayment/sdk/konaprepay/crypto/b;
Description: Use of weak cryptographic algorithm: DES

Method: DES
Class: Lcom/mastercard/api/crypto/a;
Description: Use of weak cryptographic algorithm: DES

Method: DES3
Class: Lcom/mastercard/api/crypto/a;
Description: Use of weak cryptographic algorithm: DES

Method: DESCBC
Class: Lcom/mastercard/api/crypto/a;
Description: Use of weak cryptographic algorithm: DES

Method: SHA1
Class: Lcom/mastercard/api/crypto/a;
Description: Use of weak cryptographic algorithm: SHA1

Method: getMD5
Class: Lcom/nostra13/universalimageloader/cache/disc/naming/Md5FileNameGenerator;
Description: Use of weak cryptographic algorithm: MD5

Method: <init>
Class: Ljavax/crypto/spec/DESedeKeySpec;
Description: Use of weak cryptographic algorithm: DES

Method: <init>
Class: Ljavax/crypto/spec/DESKeySpec;
Description: Use of weak cryptographic algorithm: DES

Access Control Issues

Component: com.konasl.dfs.ui.deeplink.IntentForwardingActivity
Type: activity
Description: Activity exported without proper access control

Component: com.konasl.dfs.ui.splash.SplashActivity
Type: activity
Description: Activity exported without proper access control

Component: com.facebook.CustomTabActivity
Type: activity
Description: Activity exported without proper access control

Component: com.google.android.gms.auth.api.signin.RevocationBoundService
Type: service
Description: Service exported without proper access control

Component: com.google.firebase.messaging.FirebaseMessagingService
Type: service
Description: Service exported without proper access control

Component: com.google.firebase.iid.FirebaseInstanceIdService
Type: service
Description: Service exported without proper access control

Component: konashield.security.konasl.com.konashield.security.KonaShieldService
Type: service
Description: Service exported without proper access control

Component: com.konasl.dfs.receiver.GoogleSmsReceiver
Type: receiver

Description: Receiver exported without proper access control

Component: com.google.firebase.iid.FirebaseInstanceIdReceiver
Type: receiver
Description: Receiver exported without proper access control

Component: com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver
Type: receiver
Description: Receiver exported without proper access control